Chrysostomou, Xenia (2013) Validity of the People Risk Framework: Evidence from the FSA. [Dissertation (University of Nottingham only)] (Unpublished)

Nottingham University Business School

UNITED KINGDOM · CHINA · MALAYSIA

University of Nottingham

Validity of the People Risk Framework:

Evidence from the FSA

Xenia Chrysostomou

MSc Risk Management

Validity of the People Risk Framework: Evidence from the FSA

by

Xenia Chrysostomou

2013

A Dissertation presented in part consideration for the degree of
"*MSc Risk Management*"

Abstract

The recent Global Financial Crisis was the ultimate manifestation for the recognition and appreciation of people risk, one of the dimensions constituting operational risk, highlighting the necessity of people risk management within the financial industry. In recognition of the magnitude of its impact, 'people risk' became a 'hot' topic amongst the financial regulators, which resulted in the stipulation of assigning capital reserves, exclusively dedicated to its coverage. However, the nature of people risk is attached with the impediment of broadness and diversity, which leaves operational risk managers victims of uncertainty of its unidentified boundaries. With the purpose of analysing people risk, and capturing its scope, McConnell (2008) has developed a theoretical framework consisting of four 'escalating' dimensions, namely; incident, individual, institution and industry. The aim of this paper is to examine the extent to which this theoretical framework is applicable in practice, by conducting a qualitative content analysis using the Financial Services Advisory Final Notices imposed on banks and insurance firms as evidence. The investigation attempts to find whether there is a correlation between the theoretical framework and the 'real' evidence, in order to evaluate its validity. The analysis finds that, in fact, there is evidence assuring its validity, yet there is room for improvements for more accurate outcomes. The study recommends that the framework should expand the dimensions constituting the framework. Possible suggestions are to include additional dimensions in relation to system and process risk, and the 'Three lines of defence' model.

Keywords: People Risk, People Risk Framework, Operational Risk, Operational Risk Management, Organisational Culture

Table of Contents

Acknowledgements i
1. **Introduction** 1
2. **Literature Review** 6
2.1. Introduction 6
2.2. The role of Financial Services in the Market 6
2.2.1. What Financial Institutions do 9
2.2.2. How they Operate 11
2.2.3. Comparison of Banks and Insurers 13
2.3. **The Rise of OpRisk** 16
2.3.1. Business Operations Model and OpRisk 18
2.4. OpRisk and Regulation 22
2.5. OpRisk Management and People Risk Management 26
2.6 People Risk Framework 38
3. **Methodology and Data Collection** 42
3.1. Introduction 42
3.2. Aims and Objectives 42
3.3. Method 43
3.4. Source 45
3.5. Sample Criteria 45
3.6. Data 46
3.7. Descriptive Analysis 47
3.8. Data Collection and Analysis Technique 48
4. **Findings** 50
4.1. Introduction 50
4.2. Incident 51
4.3. Individual 56
4.4. Institution 59
4.5. Industry 62
4.6. Evaluation of the Framework 64
5. **Conclusion and Recommendations** 66
6. **References** 70
7. **Appendices** 75

Appendix 1: Brief Description of the Final Notices in the sample 75
Appendix 2: Description of the Principles Breached 77
Appendix 3: Analysis of the Data- Evidence on the four Dimensions 78
Appendix 4: Reaction to an Incident 103
Appendix 5: Causes of Behaviour and Employee Intentions 104
Appendix 6: Causes of Failure at the Institution Level 105
Appendix 7: Impact of People Behaviour in the Industry 106

Acknowledgements

I would like to take this opportunity to thank all the people who have contributed in any way to the completion of this dissertation. Particularly, I would like to express the deepest appreciation to my supervisor Dr. Cormac Bryce for his guidance, support, patience and enthusiasm for the project that kept me motivated. I also want to thank my extended family and friends who supported me and kept me motivated throughout the whole process. Special thanks to Michael John Epaminondou for his invaluable assistance and support, and who helped me stay focused until the end. Finally, I want to express my deepest appreciation to my parents, Chrysostomos and Christina, for making all this possible, and to whom I dedicate this project.

Xenia Chrysostomou

1. Introduction

Operational risk (OpRisk) is the contemporary risk category which characterises the risk of losses arising from anything but credit and market risk, such as, fraud, system and process failures, natural disasters, employee errors, information losses, lawsuits and computer hacking (Moosa, 2007). OpRisk has been introduced in the financial sector as a result of the collapse of Barings Bank in 1995; even Nick Leeson, the rogue trader responsible for this collapse, has been characterised as the 'true author' and 'unwitting inventor' of OpRisk (Power, 2005). This operational loss event proved to be a 'defining moment' for the financial regulation, since it introduced OpRisk as a distinct form of financial risk, and for the first time it was required that banks should measure, manage, and allocate capital to it (Bryce, et. al, Forthcoming). However, despite the increasing awareness raised within the financial sector about the severe consequences of this type of risk, over the last decade, OpRisk management failures kept remaining the cause of major business failures and financial scandals. Inevitably, these losses which cost billions of dollars, have led to the spur of an ongoing interest paid to OpRisk by media, financial regulators, supervisors, executives, and the public. Such operational loss events include; Daiwa in 1995 and AIB in 2002 as a result of undetected illegal trading; Bernard Madoff's Ponzi scheme in 2008; Société Generale in 2008 and UBS in 2011 due to rogue trading; and PPI scandals (1990s, 2011). Even though these events have provoked regulatory developments to quantify, manage, disclose and capture OpRisk, operational losses keep surfacing across the financial industry even until today, with the GFC being the most recent, designating new deficits in OpRisk management practices in place (Sturm, 2013).

In effect, the recent Global Financial Crisis (GFC) 'shook the regulatory system'. This is because, despite the previous attempts of Basel II (the accord of banking regulation) to provide more advanced risk measures, aiming to capture OpRisk; the GFC has indicated that OpRisk was one of its 'root causes', clarifying that OpRisks were underestimated. Evidently, the regulatory framework was not strong enough to prevent systemic risk. As Bryce et al. (Forthcoming) reports, Basel II relied too much on people across the whole corporate hierarchy, which required successful training and board engaging, while individuals' perception

influenced risk culture even further. Inevitably, these failures resulted into to its replacement by Basel III, its revised version, which will take effect during the current year. Simultaneously, as a result of the GFC, Solvency II accord, the respective capital adequacy regime for the European insurance industry which is greatly based on Basel II, is currently being finalised, and will come into effect in the beginning of 2016 (Lloyds, 2013). These regulatory changes aim to improve the existing risk management models and procedures within their sector distinctively, and within the financial industry as a whole.

Under these accords, financial institutions are required to maintain a minimum capital requirement to guard against unexpected losses, while this buffer simultaneously reduces systemic risk to an 'acceptable level' (i.e. the risk that a single failure could generate additional failures along the financial system due to the interconnectedness of transactions and institutions across the industry) (Power, 2003). As a result of the globalised market, the purpose of the financial regulation is to promote international monetary and financial stability. In order to achieve these objectives, regulators try to strengthen the risk controls in the financial sector and to regulate the adequacy of the capital base by ensuring that enough capital is reserved to cover operational risks, in addition to credit and market risks, while reducing systemic risk.

The Basel Committee on Banking Supervision, the world's senior banking regulatory board, has defined OpRisk by identifying its 'root causes' (McConnell & Blacker, 2011), specifically; *'the risk of losses resulting from inadequate or failed internal processes, people and systems or, from external events'* (BCBS, 2006: p.114). This definition includes operational losses resulting from events such as damage to physical assets, legal risks, loss of data, and other factors that result in unexpected losses, except reputational and strategic risks. It also identifies several event types that are specific to people risk such as loss of key employees, internal and external fraud, and improper business practices (McConnell & Blacker, 2011). The definition implies that in order to measure OpRisk, institutions should be able to accurately assess all the dimensions of OpRisk. This paper focuses only on 'people risk' dimension. Several authors have tried to define 'people risk', however, as McConnell (2008) argues, the boundaries of this particular risk are not well defined, despite the regulatory attempts to cover people-related risks in the capital requirements. Nevertheless,

this is not surprising considering the difficulties in measuring and predicting human behaviour. Hence, without a proper understanding of this particular dimension of OpRisk (i.e. people risk), firms are unable to manage and 'accurately' assess the necessary capital requirements to safeguard from systemic risk.

Indeed, investigation of the GFC conducted by several authors (Dedu, et al., 2011; Kirkpatrick, 2009; McConnell & Blacker, 2011; Ashby, 2010) demonstrated that systemic people-related failures (incurred from individuals' actions and behaviours), in relation to both risk management and corporate governance across the whole of financial industry, were principle instigators of the outburst of the GFC[1]. People-related risks include 'problems that are related to actions, or non-actions, by individuals' (McConnell & Blacker, 2011: p.85). One of the most predominant aspects of the crisis was the human and cultural weaknesses which resulted from ill-defined values and beliefs (Ashby, 2010). However, it was indicated that these weaknesses were incubating in the organizations long before the GFC. The liquidity issues that arose in 2007 acted as the 'trigger event' for the outburst of the immense financial losses. These weaknesses have portrayed the flaws of the financial institutions, and most importantly their regulators, in providing the appropriate internal measures in managing and controlling human behaviour in their business and the financial industry in general. Thus, one of the outcomes of the financial crisis is the need of improved people-risk management. As McConnell and Blacker (2011) suggests, the role of people risk management should be formally recognised by regulators, as an independent skilled function within the risk management function, with well-defined responsibilities and protections (McConnell & Blacker, 2011: p.113). Of course, as Green (2009), the former chairman of HSBC argues, 'better risk management, enhanced regulation, codification of directors' responsibilities in company law,

[1] More precisely, it is not argued that the primary cause of the GFC was due to OpRisks or people-related issues, but rather unsustainable credit risk was the cause/evolution of the crisis that originated from the US subprime crisis that led to the collapse of major financial institutions creating solvency crisis. This caused capital markets to freeze, leading to liquidity crisis where banks and insurers were unable to fund their financial operations. These events gradually resulted in the faltering of the global economy due to the high interconnectedness amongst the financial institutions. In support of McConnell and Blacker (2011)'s argument, none of these events were caused by a single individual or a group of individuals, rather they were eventually developed and accelerated as a consequence of actions or non-actions of many trusted bankers.

and many other necessary operations, will only be sufficient with a defined culture of values.

Undoubtedly, history has revealed that the only 'common denominator' of operational loss events is human behaviour and more generally, people-related failures. McConnell (2008) states that people risks are the risks that give rise to the industry's greatest operational losses. Consequently, this evidence raises the question whether 'OpRisk management is all about managing people', and as Martin (2009) states, if this argument is true, organisational culture is the central theme in the entire debate concerning OpRisk management. Culture can be explained as 'how employees behave when no one is looking'. Nevertheless, despite the fact that since the mid 1990s OpRisk events have indicated that 'people' are responsible for nearly every operational loss event, resulting from inefficient internal controls, regulators still provide little guidance in dealing with people risk, which as McConnell (2008) described it, it is the greatest risk financial institutions are exposed to. This negligence towards people-related risks can also be emphasised by the fact that it appears only once within the main Basel II document, and only in the definition of OpRisk itself (McConnell, 2008). In addition, the document clearly refers to more than just the internal people or 'employees' of an organisation, it also recognises external fraud, however, regulators have provided little guidance as to the full scope of the term (McConnell, 2008).

Moreover, given that there is an extensive body of literature on the root cause analysis of managerial and operational losses in other sectors, there is only a limited academic research on the implications of 'people risk' or people management in the financial sector. This may be explained by two reasons; firstly, losses are not related to deadly events, and secondly, many people consider that, when they refer to organisational culture, in fact, they refer to employees. Nevertheless, financial losses and the collapse of any bank have tremendous catastrophic consequences for an economy. Additionally, there is evidence that 'people', and particularly 'managers' and 'employees', are the ones responsible for large institutional losses, while failure to capture people-related risks was proved to be the fundamental weakness of the financial system during the GFC. However, it is remarkable that there is only a limited body of research specialising merely on people risk, including identification and mitigation

techniques. Understanding its importance and identifying possible areas that these risks can potentially arise may be an important step towards managing people risks. However, in order to do so, a good starting point of this niche area in the literature would be to examine the extent to which the existing theories are compatible with reality, which will enable further development within the empirical literature.

This current paper aims to tackle this gap in the literature, by considering the extent to which the People Risk Framework, suggested by McConnell (2008) can be used by practitioners to analyse people risk, and the extent to which it captures its scope. Therefore, the validity of the framework will be tested through an investigation of the Financial Services Advisory Final Notices (FSAFN) imposed to banks and insurers, operating within the UK financial market during the last five years (2008-2012). The investigation will focus on the identification of people behaviour and actions, and the reasoning of this behaviour. The analysis will seek to find whether a correlation exists between the real-life evidence and the four escalating theoretical dimensions of people risk framework, namely; incident, individual, institution, and industry. From this analysis, it is expected that an insight will be gained regarding the scope of people risk which will facilitate the evaluation of the framework, and it will enable the researcher to spot possible improvements in relation to the framework and perhaps, in relation to the Financial Services Authority (FSA). Lastly, it is important to mention that although this paper acknowledges that FSA has been currently replaced by Financial Conduct Authority (FCA), it will be referring to the regulation as FSA since the period in which is referring to is prior to the new regulation.

The remainder of this paper is structured as follows; Section 2 discusses the background of people risk by drawing attention to the role of financial services in the market, financial regulation, OpRisk and finally, people risk. Section 3 explains the methodology employed in this research paper. Section 4 discusses the results of the analysis, and finally, Section 5 discusses concluding remarks, limitations and recommendations.

2. Literature Review

2.1. Introduction

The following section will discuss the background of 'people risk' in financial institutions by stressing the importance of the financial services in the market, how the financial institutions operate and how they are regulated domestically and internationally. Then, OpRisk will be discussed, followed by an evaluation of the existing literature of 'people risk'.

2.2. The role of Financial Services in the Market

Financial services play a substantial role in the social wellbeing and the economy in terms of growth and development, both domestically and, as a result of globalisation, internationally. Despite the increasing complexity of (relatively) new products in the financial market, traditionally, the two fundamental contributions of the financial sector are its ability to allocate resources and to manage risks (Bryce, et al., Forthcoming). The financial products they offer (i.e. banking, savings, investment, insurance, debt and equity funding, etc.) have the ability to provide profitable 'economic opportunities', including allocation and monitoring of society's savings, facilitation of risk amelioration, and trading. Essentially, they help businesses and individuals to raise funds, reduce financial uncertainties by offering risk mitigation services, save money, and build credit; while enabling the start-up or expansion of a business by plummeting vulnerability and managing their assets profitably (Sutton & Jenkins, 2007). Fundamentally, they control the well-functioning of the financial system, under which market efficiency is encouraged through improvements in capital allocation, economic growth, reduction of income inequality, and increased competition, domestically and internationally. Therefore, with their substantial expertise, reputation and geographical reach, these institutions are usually large enough to have a tremendous impact on the way the entire market operates by using deliberate strategies to expand these 'economic opportunities' through their business models. Further, due to their large size, financial institutions can enjoy economies of scale which allows them to have a comparative advantage in resource allocation and risk management, as they are able to predict the

variance on both sides of their balance sheet more accurately (Bryce, et al., Forthcoming).

In particular reference to the UK economy, the importance of the role of the financial sector can be stressed by the fact that it contributes to more than 8% of the country's GDP (TheCityUK, 2012). According to BBA (2012) and ABI (2011), banks and insurance firms dominate the UK financial services industry (Bryce, et al., Forthcoming). In addition to this, the deputy Prime Minister of the country stated that the Government's short-term plan is to rebalance the country's economy away from the overreliance on the financial sector (Gov.UK, 2011). These facts indicate how important the financial sector is for the sustainability of the UK economy. Over the last few decades, the UK financial service sector has been forced to continuously adapt to changes both in the wider economy and within the sector itself. These changes have led the financial institutions to strategically move away from their traditional business lines by undertaking more complex project or activities; a case particularly apparent during the recent GFC. This transforming environment can be traced back to the mid-80s where the UK financial system started to be extensively formalised and regulated (Moran, 1989). As a result, organisational controls and OpRisk management came forward as an 'explicit regulatory resource', thus new roles (i.e. compliance officer, OpRisk manager) were created to deal with the new demanding regulatory rules (Power, 2012).

Additionally, in 1997 the FSA was established, as the domestic supervisory regulatory body, with the aim of reducing financial crime including money-laundering, internal fraud, misuse of client assets and, maintaining market confidence. Ever since its formation, its 'overarching principle' regarding management and control is that a firm must take reasonable care to organise and control its activities responsibly, with adequate risk management systems (Power, 2012). Ayres and Braithwaite (1992) described this regulatory strategy as 'enforced self-regulation', since in order for the regulated firm to comply with this principle, they are given the authority to arrange their activities in a way that best suits their business model. Even though this regulatory strategy introduced internal control systems as a key source for this kind of regulatory style (Power, 2012), the model of substantial self-regulation, with regulators proclaiming only general rules rather than detailed ones, has been substantially

discredited as a result of the financial crisis (Schooner & Taylor, 2010). In response to these failures, the elder model of financial regulation has been reformed, and the FSA is currently being replaced by the FCA which is mostly focused on consumer protection, promoting competition in the interest of consumers and protecting and enhancing integrity of the UK financial system (Allen & Overy, 2013).

Bryce, et al., (2011) argue that FSA has shaped the way in which the UK financial institutions conduct their daily operations. In support of their argument, this can be justified considering the riskiness involved in their activities, and the substantial role they play in the well-functioning of the country's economy. However, considering the globalised nature of today's financial system, it is essential that the domestic regulation is structured in accordance with the international regulation (i.e. the Basel III and Solvency II accords). These accords aim to develop a greater insight to the trends and practices of the current financial industry, in order to supplement more powerful risk management solutions (Bryce, et al., 2011). The latest versions of these frameworks highlight the importance of OpRisk management within the sector, while directing regulatory attention on the organisational control systems and cultures of control, reflecting OpRisk as a key component of global banking and insurance regulation (Power, 2005; Hoyte, 2005).

2.2.1. What Financial Institutions do

Fundamentally, the financial system controls and manages 'credit', while it relies on individuals (or investors) to provide the funds required to acquire the resources needed (Cetina & Preda, 2005). Credit seekers are given money (resources funded by the investors) in the form of debts, which are the claims investors can make on future income and on economic output and development. These claims usually take the form of corporate shares, or bonds, which are traded in the financial market through the help of financial institutions (i.e. banks, insurers) that act as agents or financial intermediaries. Their role is to 'package the deals, assume some of the risks, and facilitate the trading of claims and risks amongst market participants' (Cetina & Preda, 2005: p.14). The existence of the financial markets is one of the major components of the 'credit mechanism in risk-based economies', as they allow the relocation and control of claims and risks amongst the participants and the relocation of wealth for capital use, while pursuing additional profits through sophisticated trading. Nevertheless, according to Cetina and Preda (2005), financial activities are a defining characteristic of the corporate economy, the welfare and social security system and, general culture.

One of the defining characteristics of the financial sector is that it is 'run on trust'; this is why market confidence is essential. This is inevitable since its products are built upon some form of financial commitment, or an 'exchange relationship', amongst the counterparties involved. The long-term nature of these financial products, their complexity, their importance to individual wellbeing, and the lack of individuals' expertise in judging the product performance, imply that customers perceive high levels of risks when making purchase decisions (AIFA, 2012). Therefore, it is important for the parties involved to be assured that their counterparty will be remaining in business and that, their financial interests are protected. Faced with such uncertainties, customers usually seek the advice on product selection (type and quality) from financial institutions. However, in consequence of the growing failures in the sector, such as the recent GFC and PPI scandal, there is an increasing concern about the extent to which these institutions are trustworthy; inducing customers to lose their trust in them. In particular, the recent PPI scandal, with the UK's largest banks being the largest distributors of these products, has had a

considerable negative impact on the financial services industry. It was estimated that the cost of the customer compensation to the UK banking sector amounted to £8 billion (Reuters, 2011). As a result, the FSA (2011) stated 'confidence in the financial services sector as a whole is at low level' (FSA, 2011a: p.15). Given the sector's importance in the market as well as the fragile characteristics in which the sector is built upon, it is not surprising that the financial sector is highly regulated, since the costs of making mistakes are considerable. Government and regulators have been keen over the years to force financial institutions to be 'prudent', however, during the GFC, financial institutions overlooked the 'basic rules of operating' and expanded their balance sheets at the 'expense of increasing risk' (Bryce, et al., Forthcoming).

2.2.2. How they Operate

2.2.2.1. Banks

Historically, banks have been the main source of financing to a vast majority of economic participants, from individuals and multinational corporations to countries, which justifies why banks collectively and individually acquire a substantial stake in the on-going economic viability of these borrowers (Teeters, 1983). In brief, banks act as intermediaries between people who want to save their money and earn some interest, and those that need money. Therefore, they earn income by selling money in the form of loans, overdrafts, certificates of deposits among other financial products, while they charge a transaction fee and an interest on loans which is lower than the interest they pay on deposit accounts. The interest rate is set according to the number of borrowers, the funds available to the bank and the LIBOR rate; the rate charged for inter-bank lending. It is also affected by the level of risk attached to the loan, in other words, the probability that the loan-holder will default. Additional income is earned by charging transaction fees when providing services to individuals and business including foreign exchange, credit/debit cards ATM access, investments and securities.

2.2.2.2. Insurance

Similarly, insurance companies provide risk management services. Their main function is to accept risks from their customers, pool them together, and manage them actively by redistributing them partly in the financial markets, and partly to reinsurers. Since claims normally will not occur all at once, the total cost of risk management is reduced for everyone in the pool. Insurance contracts involve a payment made to the insured upon the occurrence of an adverse, predetermined event (such as, car accident, natural catastrophe, health problems), in exchange for a steady stream of premiums (insurer's liabilities) paid in advance. The main services they provide include security against financial losses (theft or accident), investment services, and risk management consultation. Security is provided by transferring the risks of the insured to the insurer, where a funding upon a claim can be granted; a service particularly important for risk-averse individuals. By pooling the prepaid premiums and investing them profitably, policyholders can take advantage of the insurer's investment expertise, the reduced unit costs

(derived through the exploitation of economies of scale), as well as the spreading of the investment risks. Lastly, insurers are able to offer risk management advice. For example, when an insurance contract is signed for a property, insurers advice their customer on how risks can be reduced, i.e. reduction of theft incidents by installing security systems; in this way premiums can also be discounted. Montross (2011) argues that, well-managed insurers firstly understand that they are in the risk assuming business and as such, 'nurture' a culture that has a healthy respect for risk. Consequently, they are 'fanatical' about receiving compensation on their balance sheet, and they keep track on their assets to ensure that they do not overexpose themselves to one type of risk creating an aggregating problem.

2.2.3. Comparison of Banks and Insurers

In general, financial institutions provide strong and diversified instruments that are more manageable during periods of financial distress, whilst they provide greater stability to the financial system together with alternative funding opportunities for the borrowers. However, even though the two types of financial institutions serve two completely different aspects of the market, with insurers proving a more specific line of services, thus less exposed to risk, they are both exposed to risk in their daily operations (Al-Darwish, et al., 2011). Nonetheless, the two sectors are fundamentally different. More explicitly, insurance risk is 'idiosyncratic' and independent of the economic cycle due to the fact that claim payments occur years after they have been collected, making insurers to have stable portfolios to manage, with long-term horizon (The Geneva Association, 2010). On the other hand, banks deal with all types of contracts including short-term, long-term, liquid demand deposits, etc., therefore banks are exposed to credit and liquidity risks associated to lending activities and the mismatch from 'borrowing short and lending long'. As a result, bank-specific risks are largely influenced by the economic cycle (The Geneva Association, 2010). These differences arise from the divergence in their business models, making the nature of capital required by both institutions naturally different. In essence, the banking business model is asset driven, leveraged with a vast range of activities. Conversely, the insurance business model is liquidity driven, funded by the prepaid premiums, enabling liabilities to provide more loss absorption than banks, and consequently, inducing insurance firms to be less exposed to liquidity risks (Al-Darwish, et al., 2011). Additionally, in banking, the valuation and accounting of assets and liabilities are more retrospective than in insurance under Solvency II, implying greater firmness in the reported values for banks than for insurers (Al-Darwish, et al., 2011). Also, unlike insurers that are able to change the risk profile of their balance sheet, banks use different tools, indicating an additional difference in the way they change the risk profile of their balance sheet.

These divergences suggest the existence of the variances in the composition of the level and quality of capital amongst the two sectors (Al-Darwish, et al., 2011), while they clarify the reasons why banks are more fragile during crises than the insurance companies. The GFC indicated that insurance firms have a

more stable capital base than that of banks. This can be explained by the fact that banks are largely dependent on the wholesale market and the interbank lending, which are both built upon trust amongst them, making the banking sector to be largely affected by the changing economic environment. Consequently, these differences between the two types of institutions may justify the existence of the two distinctive regulatory accords; Basel III and Solvency II.

The European Commission suggests that the general rules of the two sectors should be compatible in order to establish consistent regulation across the financial industry, i.e. similar products in the two industries to be treated similarly, in order to avoid arbitrary opportunities in the market. However, as Gatzert and Wesker (2011) argue, due to the differences in economic and business activities, the two regulatory regimes will have to differ. Nevertheless, Solvency II is often referred to as the 'Basel II for the insurance industry' (Bryce, et al. Forthcoming) as it is built upon the Basel II three-pillar structure. The three-pillar structure refers to the following; Pillar I which focuses on modelling and sets quantitative requirements concerning capital and risk measurements; Pillar II which involves qualitative conditions of risk management such as, the supervisory activities over the institution's risk management activities, and Pillar III which focuses on disclosure requirements by regulated firms. Therefore, the two regulatory accords are built upon common grounds, and overlapping objectives, that aim to improve the quality of capital, while suggesting different requirements to common issues. Particularly, as a result of the GFC, Basel III targets an incremental enhancement of the quality and quantity of banking capital, while Solvency II concentrates on the strengthening of the policyholders' protection through 'tailoring' the quantity and quality of regulatory capital required to reflect the risks of *each* insurer, rather than raising the regulatory requirements of the sector as a whole.

Although the activities of the two sectors are partially overlapping, Al-Darwish, et al. (2011), recommends that the two accords should consider the collective allegation of the behavioural incentives that the two regimes provide, by targeting the reduction of the risk of unintended consequences associated with seemingly inconsistent treatment of the same risks under the respective accords. This may potentially avoid unintentional arbitrage between internal models and the standardised approach under Solvency II, as has happened under Basel II.

Moreover, Gatzert and Wesker (2011) who conducted a comparative assessment of the two accords concluded that, regulators should be cautious regarding regulatory bureaucracy and impediments that may encourage reduction of transparency, suggesting the importance of 'proportionality principle'. Such a principle implies that risk management, capital requirements, and reporting requirements should correspond to the risk condition of the specific institution rather that to the industry as a whole. Lastly, Ashby, et al., (2012) found evidence that bureaucracy impacts negatively the organisational culture as it imposes pressure on individuals affecting the employee morale adversely. Therefore, when setting rules and regulations, regulators should ensure that bureaucracy is kept to the minimum possible level to avoid such adverse effects.

2.3. The Rise of OpRisk

OpRisk has been around ever since the introduction of banking, however, its transforming nature throughout the years, deregulation, globalisation, the evolution of technology, and the introduction of automation on a broad scale have led to the rise of its importance, while inevitably, caught regulatory attention (Moosa, 2007; Cummins, et al., 2006; Meyer, 2000; Buchelt & Unteregger, 2004). It has been proved that recent developments in the use of e-commerce, mergers and acquisitions, complex technology, outsourcing arrangements, complicated financial assets and multinational trading procedures are responsible for the manifestation of operational losses (Cummins, et al., 2006; Moosa, 2007). Buchelt and Unteregger (2004) argue that although the risk of fraud and external events always existed, these changes have enhanced the likelihood of OpRisk loss events, and unavoidably, transformed business risk management to a key senior executive concern. In essence, these advances are responsible for the changing risk profile of the financial institutions and their exposure to OpRisk. In particular, it has increased competition and the need for cost reduction, as well as improved risk-based decision making (Ashby, 2008), thus explaining the reason why the concept of OpRisk was transformed from 'anything other than market and credit risk' to one of the three principal risk categories faced by the financial institutions (i.e. credit risk, market risk, and OpRisk). In fact, the Basel Committee on Banking Supervision proposed the incorporation of OpRisk to allocate the necessary resources to guard against systemic risk and introduced more advanced guiding principles for the OpRisk management.

Despite the regulatory conversions, technological advances and financial innovation facilitate sophisticated risk measures and management practices while simultaneously, they accommodate even more sophisticated risk exposures. More explicitly, Buchelt and Unteregger (2004) argue that the changing nature and the degree of complexity generated by the sophisticated procedures create inexhaustible potential for errors and breakdowns of all types misguiding the employees to make more mistakes, the more complex their tasks are. As Dowd (2006) argues, greater sophistication generates; greater complexity (greater scope for error), less transparency (enabling errors harder to detect), and

greater dependence on assumptions (any of which may be faulty), hence causing over-reliance and underestimation of using such systems.

Additionally, in many cases credit and market risks may be eliminated by these advances, however, new OpRisk exposures are created making it challenging to take the appropriate precautionary measures due to their unknown nature. This is the reason why there is an increasing concern in the literature on how to tackle OpRisk. Attempts to decrease market and credit risk have given rise to this contemporary type of risk. Such risks include system incompatibility, system failure, integration problems, risk of fraud etc. Nevertheless, exploiting and keeping up-to-date with technological advances are essential tools for the survival of financial institutions in the market. According to Meyer (2000), financial models and tools, and the environment in which they operate need to be managed and controlled, otherwise sophisticated risk management techniques are useless if their operating environment and management incentives are inefficient, or if fundamental risk management policies are ignored. Therefore, to remain competitive, it is necessary that institutions keep pace with market innovations, and constantly adapt and improve their processes, whilst paying attention to the possible areas that OpRisks may raise.

2.3.1. Business Operations Model and OpRisk

This sub-section attempts to analyse the business operations model of financial institutions in order to identify possible areas that OpRisk may occur, in order to be able to appreciate how financial regulation deals with OpRisk. To begin with, the model of the process is divided in two operational levels, the primary business environment, and the consecutive, support and control functions level as indicated in Figure 1. The primary business level consists of two distinctive areas; revenue generation, where the trading takes place through the front office, and processing activities, where front office support is provided before and after the transaction settlement. Then, support and control function follows, which comprises of 7 different compliance functions (Figure 1) that aim at monitoring and controlling the primary business level.

Figure 1 Business Operation Model

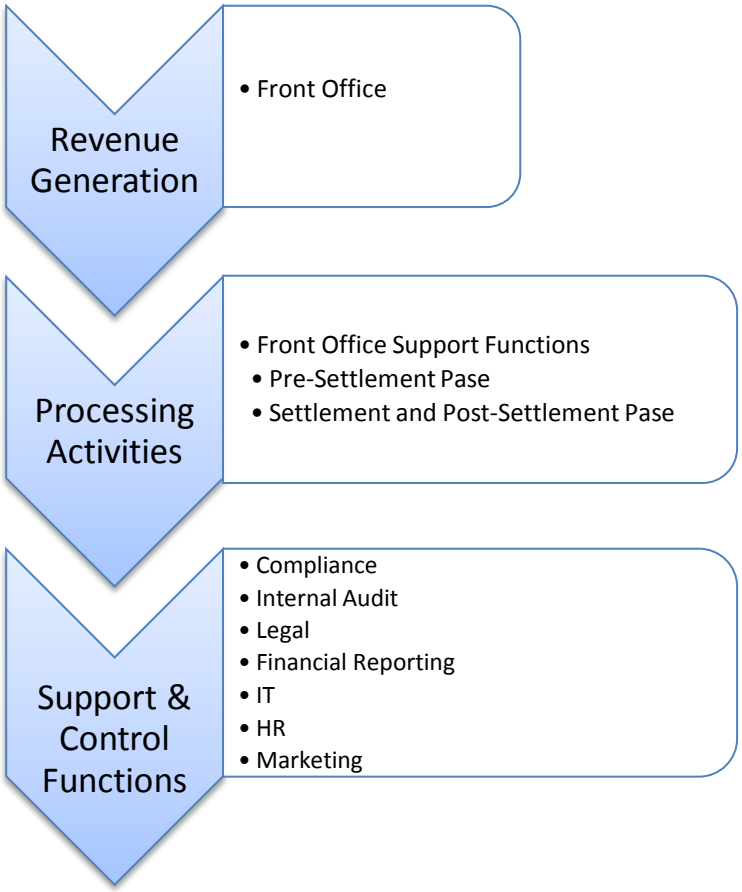


Figure 2 and 3 (below) analyse each of the two operational levels respectively, including information about tasks, types of possible OpRisks, and effective control procedures at the primary level (see Figure 2) for each department, distinctively. As the diagrams indicate, the possibility of loss arising from OpRisks exists in every operational level, while a failure occurring at any department affect the whole process since everything is interrelated, resulting into a 'chain of causation'. However, in order to reduce the risks of such failures, it is essential to ensure that the front office operations are successfully operating, as they conduct customers directly and they are the first line of the business operations. In fact, history has indicated that some of the most serious operational losses have occurred at this level, such as fraud, commonly pursued by rogue traders (see Barings Bank, Société Générale, UBS). Therefore, the role of the front office support functions plays a substantial role in the process at the operational level, which further stresses the importance of the advanced level of the hierarchy (i.e. the support and control functions, see Figure 3), which is responsible to ensure that every operational line is operating according to the strategic plan. Consequently, any failure occurring at any part of the process affects the whole business model.

Figure 2 Process at the Primary Business Level

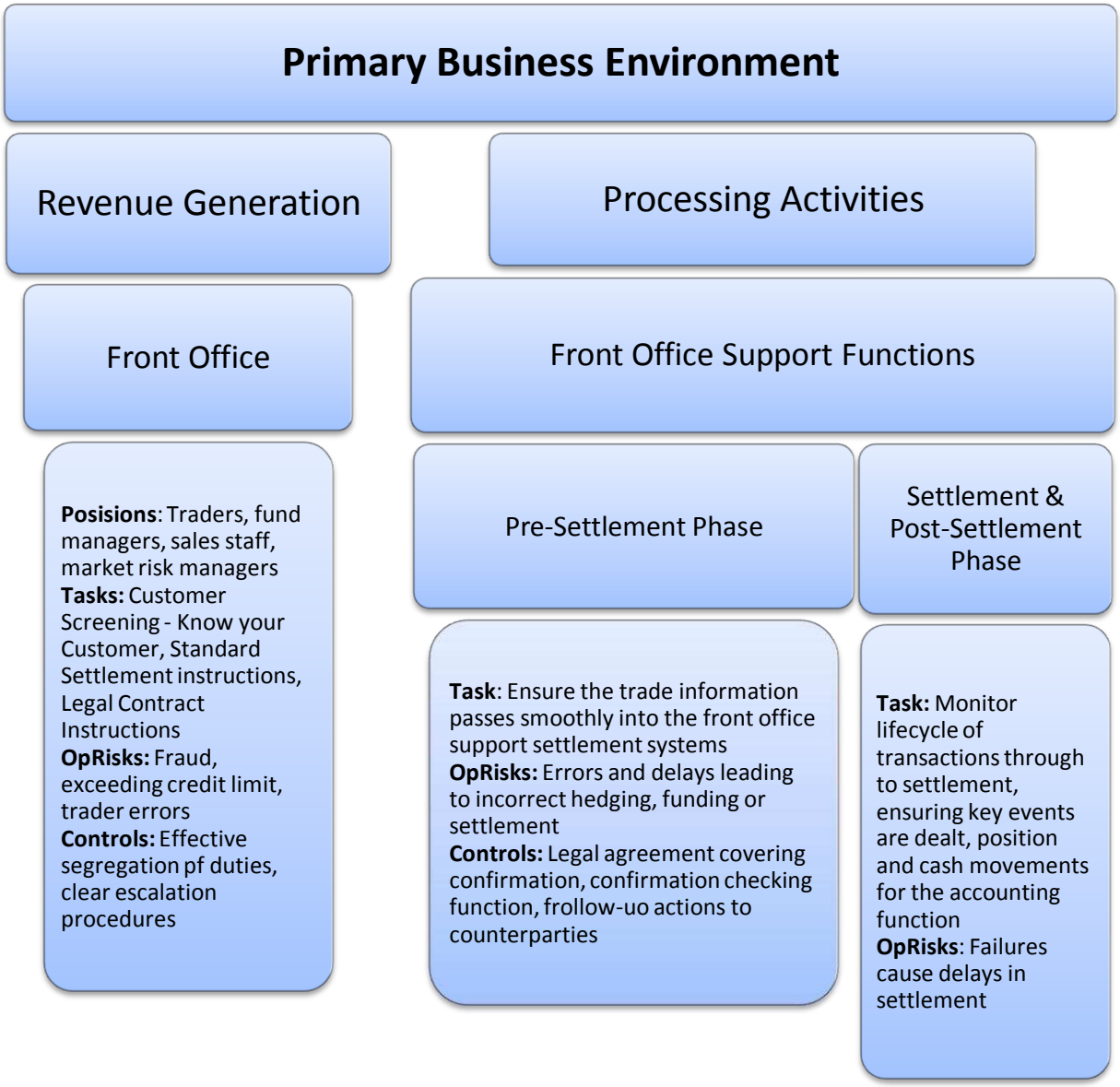
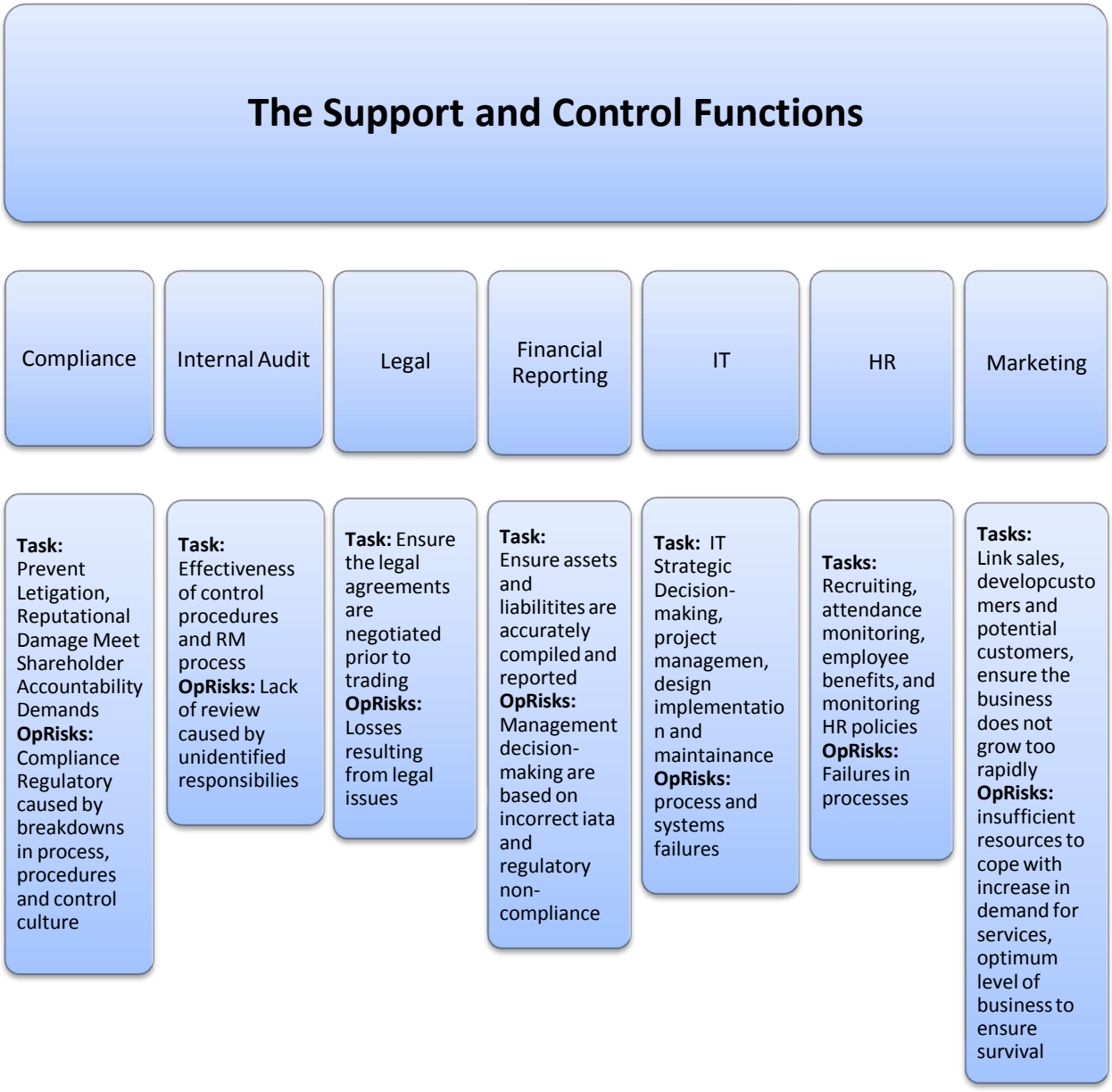


Figure 3 Support and Control Functions



2.4. OpRisk and Regulation

With the evolution of technology and globalisation, and the increased regulatory attention to OpRisk, it was inevitable that regulation will take the appropriate actions to include OpRisk in its regulatory framework. Therefore, to guide organisations in measuring the OpRisk capital requirements, Basel II introduced three approaches, namely; basic indicator, standardised, and advanced measurement, with the latter requiring the highest level of capital reserves. Each of them requires different levels of capital and different sophisticated levels of risk management to calculate the risk-based capital with respect to OpRisk, using domestic OpRisk metrics such as, internal and external loss data, scenario analysis, and risk mitigation techniques (i.e. KRIs[2]). The accuracy of such a technique in predicting the future losses is based on the volume and quality of acquired information, inducing institutions to adopt the Loss Distribution Approach, where the 'capital requirements are set according to a historical database of operational loss events involving frequency and severity of losses' (Bryce, et al., 2011: p.1163). Hence, this approach requires reporting of any internal or external operational loss event developed within a learning environment along with 'no blame' culture. More explicitly, learning environment refers to organisations being able to integrate lessons learned from past events in their organisational culture to avoid similar loss incidents. 'No blame' culture refers to the encouragement of reporting accidents, 'near misses', and any other failure by employees, without being afraid of losing their job if the incident is somehow related to them.

There is a debate across the empirical literature concerning the choice of the most suitable model and statistical approach to capture OpRisk, whilst setting the capital based requirement attached to each of these approaches has become a controversial issue amongst researchers. These debates arise due to the fact that domestic regulators allow flexibility in the choice of internal measures (Bryce, et al. Forthcoming). The following extract enclosed in the Goldman Sachs International Final Notice (2010) emphasises this statement, by arguing that although firms are allowed to organise their business in a way that its compliance function is responsible for regulatory notifications, senior managers are obligated

[2] Key Risks Indicators (KRIs)

to notify the FSA about any related matter. It also stresses the importance of having adequate systems and controls with senior managers responsible for their effectives while ensuring the escalation of information across the business levels;

'...systems and controls in place are required to ensure that relevant information is shared appropriately and timely within their global legal and compliance functions...to ensure that the potential impact of overseas regulatory investigations is duly considered and local regulatory obligations are duly complied with...to ensure that the business...can be properly organised and controlled. While it is appropriate to organise a firm in such a way that its compliance function is responsible for making regulatory notifications, the FSA expects...senior managers, who become aware of a matter...to focus on the need for the firm to comply with its regulatory reporting obligations and to ensure that those responsible for...reporting obligations are properly informed of the information they need to know. Senior management must take responsibility for ensuring that the firm has effective systems in place to enable it to communicate promptly and appropriately all information of which the FSA would reasonably expect notice. Communication failures arising as a consequence of group structures or procedural deficiencies will neither excuse nor mitigate failures by firms to comply with that responsibility.' (FSA, 2010: p.19)

The FSA has also provided a Handbook guidance, and other supporting materials, to supplement the principles and rules with the purpose to guide firms in choosing models and procedures that best suit their business models, and to illustrate ways in which institutions can comply with the relevant rules (FSA, 2011b). Yet, irrespective of the OpRisk management strategy adopted, institutions need to achieve a range of proportionate general risk management standards depending on the institution's size, nature, scale and complexity. Further, the BIPRU[3] entails financial institutions to acquire a well-documented assessment and management system, with transparent reporting lines and responsibility subject to a regular independent audit (FSA, 2011b). However, despite the regulatory attempts to mitigate operational losses, the banking regulation has been greatly criticised as it was proved that its effectiveness is

[3] BPRU: Prudential Sourcebook for Banks, Building societies and Investment firms

subject to failure due to its over-reliance on people's decisions and actions which are often subject to individuals' own judgement.

Many authors argue that regulators failed to give much emphasis on all of the three regulatory Pillars, thus failed to effectively capture the key areas that give rise to risk exposures. Recently, it was revealed that banking and insurance sectors have become greatly dependent on quantitative models during the last thirty years (Dedu, et al., 2011; Tuckett, 2009; Montross, 2011; Dowd, 2006). It has been argued that a possible explanation to most of risk management issues is that inadequate attention was given to the qualitative part of risk management, which requires both subjective judgement and past experience. Particularly, regulators have focused on Pillar I, the quantitative modelling, instead of Pillar II, which is the more qualitative approach to risk management. Tad Montross, the Chairman and CEO of GenRe, explains that this regulatory inefficiency is a result of the ill-defined grounds that the regulatory framework is built upon. For this reason, he also expects that there will be a debate on Solvency III to address the 'unintended consequences of Solvency II', in several years (Montross, 2011). Since Solvency II is built based on Basell II/III grounds, this statement also refers to Basel III too. His argument is that Solvency II may 'obscure' or minimize certain types of risks and leave the industry exposed to a crisis 'similar to what the banks just experienced'. The issue is that although Basel III imposes stricter and more 'onerous' capital changes and requirements, it is unclear whether risk will be better understood and managed (Montross, 2011). Consequently, further negative effects may occur, since banks will be keen on moving into riskier assets as they will be earning lower ROE[4] due to the higher capital reserves (Montross, 2011).

Additionally, Martin (2009) argues that it was evident that the regulatory requirements failed, in that they placed capital as a 'front line of defence' against OpRisk rather than the 'last line of defence'. Martin (2009), Ashby (2009), and Blunden and Thirlwell (2010) support that proactive management and prevention of OpRisk is much more valuable than measuring the losses after they occur, justifying the failure of the regulatory committee in tackling OpRisk. Therefore,

[4] Return on Equity

regulation should encourage institutions to focus on developing a deeper understanding of risks, rather than building complex models (Montross, 2011).

Furthermore, the risk management tools, such as VaR[5], that these approaches use to calculate risk and manage capital reserves, are greatly criticised by many researchers since they fail to consider the behavioural risks. Particularly, Dedu, et al., (2011) argue that uncertainty and risks cannot be managed without accounting for the 'emotional part' of the decision making process; imagination, desire, behavioural biases like herding, confirmation etc. As Tuckett (2009) states, financial markets will always tend to be subject to greed, over-excitement, anxiety, panic and divided states of mind; therefore, the sophisticated economic and financial modelling will always be subject to bias and will continue to 'create the impression that risk is being managed'.

Moreover, Bryce et al. (Forthcoming) reports that the effectiveness of Basel II was subject to the reliance upon people for effective decision making; the importance of good training for empowering of staff; the importance of board level engagement; and the individuals' own views and perceptions that influenced the implementation of organisational structure. Thus, taking into consideration the delicacy of the effectiveness of the regulation including, the lack of providing 'employee management' guidance by the regulators, it is no surprise that human-related failures dominated the real causes of the financial crisis.

[5] Value at Risk

2.5. OpRisk Management and People Risk Management

Ever since the creation of the banking industry, risk-taking is an integral part of its business and unsurprisingly, banks have been practising risk management procedures since then (Meyer, 2000). Indeed, the industry would not have survived without it, considering the fact that risk does not always have a negative impact rather, it creates opportunities too. However, considering the importance of the financial institutions in the well-functioning of the financial system, it is implied that such institutions have little, or no, tolerance for loss. Therefore, dynamic risk management mechanisms are mandatory, targeting efficient allocation of resources; initially financial resources, but ultimately real resources, to their most efficient use (Meyer, 2000). Of course, risk management is costly in both resources and 'institutional disruption', and yet, costs of ignoring (proper) risk management can have a wide spectrum of tremendous negative effects; from the failure of a particular institution in terms of loss of money or reputation, to the failure of the banking system (contagion effect).

Consequently, understanding and preventing risks from occurring (loss in the form of money and reputation) has become a key corporate objective and simultaneously, the focus of regulatory frameworks. In doing so, it was conventionally believed that organisations should aim to develop a corporate risk culture that proactively focuses on company-wide risk management that empowers all employees, at all hierarchical levels, to make decisions where necessary. However, Bryce, et al. (2013) found evidence that 'over-reliance on employee empowerment and autonomy, as a means by which to improve transparency, and risk escalation is no guarantee of a more robust risk function' (p.24). This type of strategy is directly linked to OpRisk management and as these researchers also argue; failure in education and training can be deemed as a 'precursor' of people risk. Subsequently, such arguments lead to the implication of Blunden and Thirlwell (2010) that state, 'just as risk is as much about opportunities as threats, so the people are also the greatest potential liability' (p.270), and yet, firms rarely consider people management in their risk management strategy.

The definition of OpRisk has been criticised as 'too broad' and it has been characterised as the most diverse risk category which justifies the difficulty in

limiting the number of dimensions required to describe it. Unsurprisingly, there is a lot of dispute amongst academics and professionals about the concept of OpRisk, its causes, consequences, characteristics, and management (Moosa, 2007). In particular reference to the OpRisk management, Blunden (2003) argues that OpRisk is as likely to bring a company down as a market collapse, while more often than not, failure is generated through misconceptions within management control (Moosa, 2007). Martin (2009) argues that major OpRisk events demonstrate failures in the organisational culture, with evidence on management ignoring indicators and metrics that link to a problem, or turning a 'blind eye' to a questionable business practice. As it was indicated in the Société Générale 2008 rogue trading scandal, failures in the organisational risk culture cause devastating consequences such as; fraud, safety breaches, operational disasters, and over leveraging; originating from flaws in uniqe organisational cultures (Levy, et al., 2010) and internal controls, that allowed particular risks to take root and grow.

IIF (2009) argue that, for effective risk management to be implemented, 'cultivation' of consistent risk culture is perhaps the most fundamental tool, while risk management is a key tool supporting, particularly, the OpRisk managers to accomplish corporate objectives (OeNB & FMA, 2006). They also support that, there is a close relationship between the firm's strategic orientation and the risk policy, all of which have a strong impact on corporate culture, and thus on values, opinions and attitude of employees. Similarly, OECD (2004) state that risk policy is closely related to the corporate strategy, an area of increasing importance for boards. The board must decide which risks to transfer and which to avoid, while risks, such as operational, can be eliminated through insurance, diversification and internal controls. Risk policy acts as a 'crucial guideline' for risk management in order to achieve the company's desired risk profile, thus its purpose is to specify the risk appetite of the company (OECD, 2004). According to OeNB and FMA (2006), the decisive component in creating a well-balanced interaction between these elements is to fully-embrace OpRisk management in all employee day-to-day work, which will be achieved by ensuring that 'people are doing the right thing, at the right time, and doing it consistently well' (Martin, 2009: p.82).

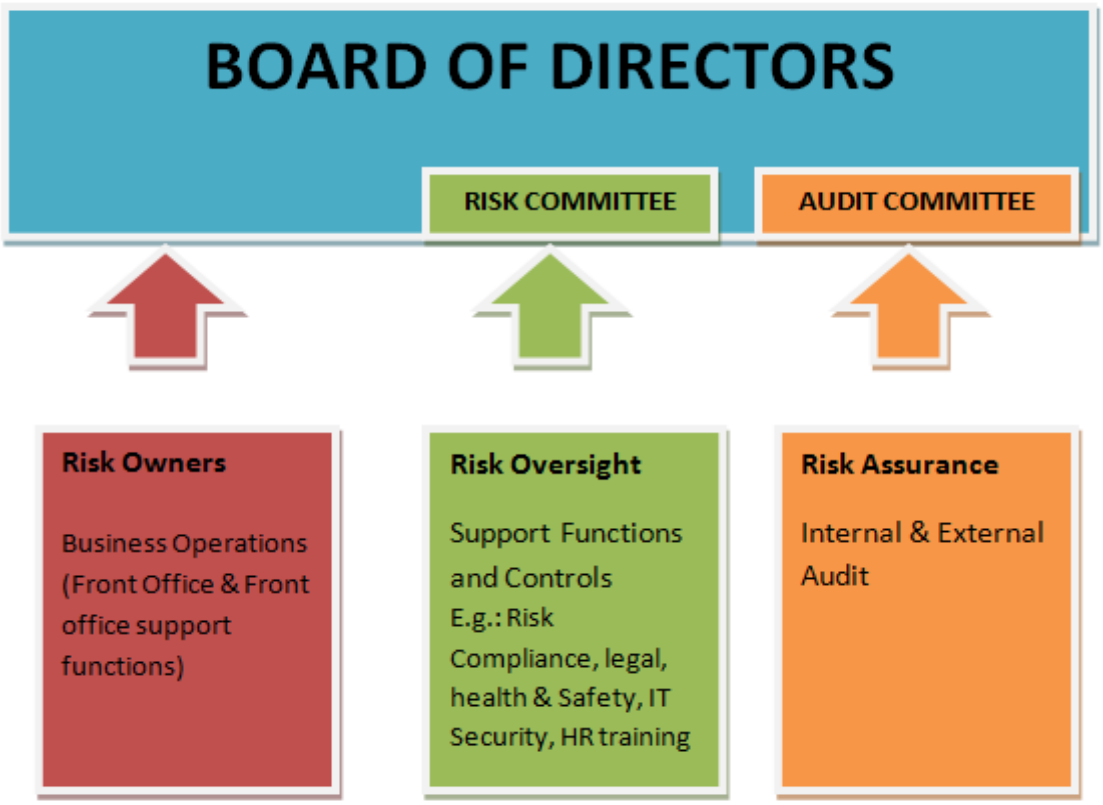
The recent market turbulence proved that effective cultivation of risk culture across institutions is the main tool that enables effective risk management (IFF, 2008). Risk culture refers to 'the norms of behaviour of individuals and groups within an organisation that determine the collective ability to identify and understand, openly discuss, and act on the organisation's current and future risks' (IIF, 2009). In other words, risk culture aims at establishing a common set of values, beliefs, standards and disciplines which define consistent approaches to risk-taking across the organisation. The implementation of a 'firm-wide focus' on risk is the task of corporate governance. According to IFF (2008) every institution should clarify that senior management and particularly, the CEO, are responsible for the following risk management procedures; to establish the board's essential oversight role in risk management, to develop a robust risk culture embedded in accordance to the firm's operations while covering all areas and activities, and to ensure that accountability for risk management is being a priority for the whole institution.

Essentially, organisational culture, its values, and valued behaviours will underpin its risk culture (IOR, 2010). Such behaviour that will provide support for an efficient risk management includes; clarity, openness, trust, honesty and integrity. These attributes encourage 'comprehensive risk reporting' which provides a challenge for the senior management in encouraging the reporting of (potentially) emerging risks, or already known risks. As Bryce, et al., (2011) argue, such information is crucial for the risk measurement and the setting of the capital requirements. Moreover, operating within such a culture reduces groupthink as people will be aware of potential risks in their operations and it will encourage successful decision-making. Turner (1994) who examined the 'causes of disaster' in an organisation, argues that implementation of such culture is crucial, since is reduces 'sloppy management'. In addition, employees at the front-row have more knowledge concerning the risks and failures of the operations, while senior management is the one responsible for decision making. Therefore, institutions should be open to 'learning' and 'challenge' while they should accommodate a 'no blame' culture that will encourage reporting of 'near misses' and failures across the organisation. As IOR (2010) argues, risk management is about being aware of the firm's changing internal and external

environment, therefore culture should be one which is active to change and continuous improvement in all aspects of risk management.

Given that the execution of risk management policies involves personnel at every organisational level, risk culture is placed 'at the heart of the human decisions' that take place on the routine activities in every organisation, and in every hierarchical level. Rationally speaking, it is people that are running the business; therefore internal controls, employee incentive schemes, and satisfaction in the working environment are vital factors for achieving the corporate objectives. Moeller (2007) describes 'internal control' as a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories; effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations (Moeller, 2007: p.4). However, instead of focusing solely on internal controls in relation to financial reporting and on the need to have external checks and reporting, as it was traditionally conceived, Kirkpatrick (2009) stresses the importance of considering internal controls as a 'subset' of risk management, which is a key concern of corporate governance. On the same lines, IOR (2010) proposed a comprehensive risk management framework depicting a clear understanding of 'risk roles and responsibilities' represented by the 'three lines of defence' approach, as shown in Figure 4.

Figure 4 The Three Lines of Defence Model



This approach outlines common 'guidelines' for the governance of OpRisk management within financial institutions. The first line-of-defence is concerned with the daily risk management in accordance with agreed risk policies, appetite, and controls at the operational level (see Section 2.3.1, Figure 2). The second line-of-defence deals with the execution of these policies, processes, procedures, and controls (see Section 2.3.1, Figure 3). The third line-of-defence is the 'independent review' (audit or risk assurance), which serves as a 'challenge function' for the other two lines-of-defence (BIS, 2011; Bryce, et al., 2013; IOR, 2010). According to BIS (2011), risk governance of financial institutions should be tailored according to their size, business model and its complexity, while the implementation of the three lines-of-defence approach varies according to their risk management approach, and the flexibility provided by national supervisors. The FSA (2011b) comments that a strong risk culture, good communication and understanding, and a strong sense of risk awareness 'can provide comfort when used in conjunction with this approach' (p.14).

In contrast with BCBS (2006), McConnell (2008), and Blunden and Thirlwell (2010), Ashby (2008) argues that, the 'root causes' of most operational loss

events are not people, processes, systems or external events, instead, they are 'organisational and social in nature' and that, they are the result of multiple interrelating factors rather than, a single cause. His argument is based on Turner (1976; 1994; 1991)'s view on disasters; unless disasters arise from natural forces, they are not created overnight. Additionally, Ashby (2008) suggests that OpRisk management is more than a simple loss prevention or financial loss reduction through insurance and capital provision, rather, such activities should be balanced by an 'appropriate investment in resilience', which aims to ensure that once losses arise, the organisation is able to accommodate them with the minimum amount of cost and disruption. He also supports that it is necessary to consider the organisational and social factors that underlie the factors which precede a loss event, such as; organisational structure and the associated management systems; management risk perceptions; organisational social culture and/or social subgroup within the organisation; internal politics and power dynamics; organisational change; external, social, political and economic pressures. Therefore, despite the alternative views on the causes of OpRisk, he concludes that losses arise from a 'chain of events' that escalate in the organisation over time, thus these losses are essentially 'man made'.

Martin (2009) argues that at the heart of most OpRisk events it is indicated that 'people failure' is always the problem, raising the question whether OpRisk is solely about managing people. Similarly, Blunden and Thirlwell (2010) add that OpRisks are ultimately the result of people failure, whether at a strategic, managerial, or operational level, by identifying two sides of people risks; employees and their managers. They explain that employees are essentially honest, however, factors such as lack of competence, training experience, and personal or domestic environment (i.e. relationships, health, economic condition) can potentially affect their behaviour and hence, their reliability. Additionally, they support that since it is difficult to assess the organisation's exposure to people-related risks, because people's personal circumstances change continuously, it is necessary to effectively manage employee risk. This suggestion is directly linked to the 'other side of people risk' – managers.

According to Blunden and Thirlwell (2010), the greatest challenges of management are to 'retain the best people and that, all perform to their best ability', which can be possibly tackled by establishing the right environment

which will include; clarification of the meaning of 'excellence' and 'good performance', that will define the organisational culture; leadership and hierarchical clarification; openness and transparency; effective management, and change and flexibility. As a subsequent result of the GFC, Martin (2009) suggests that there is a need for senior management to 'set a good example', a strategy which clearly failed during the recent crisis. Undoubtedly, establishing an effective corporate governance and risk management structure is very challenging for the senior managers, however as the FSA (2011b) advices them, the key considerations are firm-wide behaviour, engagement, and risk culture, which are the direct and active ingredients to support them.

Furthermore, Blunden and Thirlwell (2010) support that once the right environment is established, people risks can be mitigated through the selection process, appraisal and performance management, training and development, reward system, staff retention and succession planning. Meyer (2000) suggests that when developing risk management procedures, managers should focus on developing and/or attracting personnel with the skills required applying risk management tools meaningfully. Therefore, HR department plays a substantial role in the organisation, while active support is required for HR experts to resolve 'lack of training' or 'understaffing'. McConnell (2008) adds that techniques such as Six Sigma, and KRIs in conjunction with HR, are essential mechanisms to uncover 'operational quality' (i.e. employee satisfaction/turnover, etc.) and subsequently, to alert OpRisk managers by revealing problematic areas. McConnell (2008) concluded that people risks cannot be controlled by a single discipline due to its diverse scope. Therefore, he suggested that well-trained OpRisk managers should reach out to other disciplines, in particular; HR, compliance and strategic planning, to cooperate in effectively encompassing 'the full dearth of people risk'. Similarly, Ashby (2008) supports that there are many useful lessons to be learned from other sectors in providing solutions to enhance the effectiveness of OpRisk management frameworks in the financial industry.

Bryce et al. (Forthcoming) stress the importance of qualitative and quantitative training, and educational development perspective. They found evidence that, both attitude and information uncertainty endorsed by training and education on risk management process and procedures can potentially act as fundamental building blocks of a coherent and effective risk culture, and therefore risk

management strategy. Additionally, Martin (2009) and McConnell (2008) suggest that to be effective, OpRisk managers are required to pursue a 'leadership role' within the business, with acquired status and authority to provide guidance when required and also, to cease any inappropriate actions when uncovered. He adds that communication should be embedded within the whole business, and carried by the OpRisk managers by their on-site presence, emphasising the importance of face-to-face communication. However, success requires non-executives to have a clear understanding of the organizational structure, culture and risk profile, which can be achieved through training on risk matters, and company orientation (Martin, 2009).

Martin (2009) also stresses the importance of the role of remuneration policies in incentivizing particular types of behaviour. For example, recent instances have shown that, in contrast to the long-term profitability, short-term remuneration policies (i.e. volume and turnover) encourage 'misaligned incentives' between the firm's objectives and its managers. A vast body of evidence (Cihák, et al., 2013; McConnell & Blacker, 2011; Ashby, 2009) supports that 'misaligned incentives' is one of the fundamental causes of the GFC as it has encouraged bank managers to keenly boost short-term profits and create banks that are 'too big to fail', regulators to tolerate withhold information from other equally important parties and, credit rating agencies to falsely rate subprime assets. Cihák, et al., (2013) recommend 'incentive audits' as a potential solution to identify incentive misalignments in the financial industry and hence, mitigate systemic risks. Particularly, the aim of their research is to 're-orient' financial regulation towards the aim of addressing incentives on an on-going basis.

Further, Meyer (2000) stresses the importance of 'making risk matter to owners and managers' while suggesting specific prerequisites to encourage them to pay attention to risk. These prerequisites include effective risk assessment and management, which require solid accounting and disclosure standards to induce bankers and insurers to make accurate customer performance screening. In addition, due to the importance of trustworthiness, accuracy is further reinforced by auditing systems and legal penalties for providing 'fraudulent or misleading' information. In consequence, staff with sufficient expertise in identifying, evaluating and managing such risks is necessary. The absence of 'implicit or explicit government guarantees' on job security is an additional prerequisite,

where the fear of losing their job, as a result of merger and acquisitions, acts as an incentive to manage risk and avoid insolvency. Similarly, for market discipline to be effective, creditors should 'fear' run on risk of loss on their claims on banks, to incentivise banks to control such risks. Of course, to maintain market discipline 'adequate accounting' and 'disclosure standards' to enable investors' judgment on bank's condition are required, which necessitates regulatory bank supervision (Meyer, 2000). Still, accurate assessment on banks' condition, authority to close down insolvent banks, and remove inefficient management are essential to impose control on the executives and the board, thus depicting the importance of government intervention.

In effect, lack of effective market discipline was apparent during the recent GFC. Cihák, et al. (2013) explain this phenomenon as a result of 'herding behaviour' and 'moral hazard', both of which dominated the global markets. Evidently, prior to the crisis, managers of large financial institutions had expressed hazardous behaviour as a result of being treated as 'too-big-to-fail' institutions, enjoying favourable regulatory treatment (Rajan, 2010; Ötker-Robe, et al., 2011; Goldstein & Véron, 2011; World Bank, 2012). This implies that solvency of these institutions was guaranteed, because a failure of such institutions poses systemic failures in the markets. Therefore, managers were incentivised to undertake aggressive strategies irrespective of the associated risks to boost their profits, hence emphasising Meyer (2000)'s prerequisite conditions. Other examples of moral hazard behaviour inhibiting in the financial sector include; agents falsifying documents, and lying to people about the real cost of the mortgages as a result of information asymmetry.

According to McConnell and Blacker (2011), in the definition of OpRisk, losses resulting from instances of moral hazard would be classified as 'people risk', particularly, under the 'event type category' of 'clients, products and business practices'. McConnell (2008) argues that the definition covers 'people risk' beyond such intentional misbehaviours, such as; incompetence (i.e. use of inappropriate models), negligence (i.e. lack of appropriate action), lack of knowledge, usually resulting from improperly trained staff, or lack of experience and, lack of accountability resulting from ill-defined responsibilities and aggression (i.e. improper use of power). Unfortunately, these risks are hardly identified between them and in many situations, 'identical behaviour by an

individual (usually junior) can result in dismissal, but be tolerated if perpetrated by another, more senior, individual' (McConnell & Blacker, 2011: p.92). History has also revealed that, negligence towards inappropriate behaviour, leads to unethical actions, and subsequently, to illegal activities which end up into in severe losses (see Barings, National Australia Bank and Daiwa).

Further, evidence has shown that in most of these cases, managers were aware of their inferiors' illegal actions, however no action was taken when these actions were highly profitable. This is a common feature of rogue trading. In his interview, Nick Leeson admitted that although a rogue trader is a criminal, the underlying bank is also partly to blame, as such an event indicates the failings of the organisation and its flaws in its operations (cited in Watkins, 2013). Others argue that where 'the bosses knew', rogue traders may be dismissed. As Watkins (2013) argue, the role that banks play in fostering rogues is to do with corporate culture. In support of his statement, Turner (1976) states that rarely an individual or a single error has the potential of creating a disasterous outcome in a field which is believed to be 'secured', unless 'unwitting assistance' is offered by access to the resources of large organisations, and time. If this is the case then it is implied that organisational culture is inefficient. Hence, these events highlight the need for a better understanding and control of OpRisk, while they draw attention to the likelihood to fall victim to fraudulent employee in any organisation with poor supervision and management.

It is apparent that the losses incurred during the GFC exhibit perfectly all the possible dimensions of people risk. Kirkpatrick (2009) stresses that failures and weaknesses in corporate governance arrangements are largely responsible for the outburst of the crisis, since they fail to control against excessive risk-taking in a number of financial institutions. This was the result of failures in information flow about risk exposures across the organisational hierarchies, while it was evident that risk management was often 'activity-based rather than enterprise-based' which meant that key risks were unidentified and ineffectively managed. Additional failures include; non-disclosures about foreseeable risk factors, lack of monitoring and risk management systems, insufficient accounting standards and regulatory requirements, and misaligned remuneration systems. Since setting, reviewing and guiding risk policy is a key function of the board, these malfunctions signify ineffective corporate governance (Kirkpatrick, 2009).

Dedu, et al. (2011) conducted a behavioural approach to the financial crisis using the three-pillar-approach, in order to examine the 'collapse of ethical behaviour', and its role in finance in terms of, studying, regulating, and assessing financial risks. They concluded that regulatory accords will be more effective if they integrate biases of human behaviour in their frameworks, as will enable people to become less 'financially vulnerable'. In accordance with the findings of McConnell & Blacker (2011), Dedu, et al. (2011) detected the following behavioural factors (under pillar 1); optimism, wishful thinking, overconfidence, greed (salaries/bonuses), regret, pessimism, apathy (i.e. passing the responsibility), herding-groupthink, anchoring, representativeness biases, loyalty to the firm, and informational cascades. Then, they examined the collapse of ethical behaviour that led to the GFC such as, predatory lending practices, inappropriate compensation schemes, rating agencies behaviour, corporate governance reforms and financial institutions opacity in their reporting (pillar 2). Finally, pillar 3 presents the 'mismanagement of risk and regulations'. Moreover, Ashby (2009) in his 'Response to Turner Review' recommends that, in order for financial institutions to be better prepared when crises occur and be able to prevent them, the regulatory focus should be upon raising risk management standards, and creating the right incentives for managers and stakeholders. He also argues that, in order for the all the regulators (internationally) to be part of the 'solution', they should develop regulatory responses that simultaneously enhance the effectiveness of market forces *within* the financial services sector, and board/management decision-making, rather than, working against them.

To sum up, people are the heart of every organisation hence it is their individual and collective actions and behaviours that generate organisational results. However, given that actions and behaviours can be influenced by countless of factors, organisational culture becomes a necessary tool in controlling this random behaviour. In this case, the root cause analysis of severe past events is valuable, as it generates lessons to be learned and raises awareness of past behaviour and actions enabling practitioners to avoid them, whenever possible. Furthermore, considering the diverse nature of OpRisk and the highly correlated set of risks that originate distinctively across the whole organisational hierarchy, it is no surprise that cultural risk dominated the discussion. Subsequently, when referring to OpRisk, corporate culture, and more precisely risk culture, is the

main component of the overarching term which essentially refers to employees. The management of such a ubiquitous risk is a managerial task and must be performed on a broad organisational basis with the support of senior managers, and through successful communication and information flow across every organisational department. However, prior to dealing with OpRisk, people risk has to be understood and people management to be implemented with the aid of several supportive control functions, particularly; audit, supervision, effective communication, 'no blame' culture, financial reporting and HR.

2.6 People Risk Framework

Defining people risk is very challenging due to its diversified nature and its unpredictability as it is heavily based on human behaviour. In fact, there is a gap in the literature in defining and addressing people risk directly. Even regulators have been 'reticent' in defining precisely what 'people risk' covers and without a clear understanding of what constitutes people risk, there is only 'little hope' in defining, assessing, and mitigating such risks. For this reason, firms are unable to take the appropriate measures to mitigate people risks, affecting the capital requirements left aside to cover unexpected operational risk events, required by Basel II/III. Many authors have tried to explain people risk by addressing various types of human behaviour that may cause negative effects on the organisation, while others, indirectly address people risk through organisational culture which impacts employee behaviour (see Section 2.5).

However, these definitions concentrate on internal people risk, and as McConnell (2008) argues, clearly the definition of Basel II on people risk refers to external risk factors too. Thus, he stresses the importance of considering the external risks that arise due to unethical or illegal activities across the industry when dealing with OpRisk management. External people risk factors most commonly occur from customer behaviour, such as, falsified information provided by the customers in terms of, their credit profile upon entering a contract, counterparty default risks and, the risk of customers lying when submitting insurance claims. Therefore, broadly speaking, 'people risk' could be defined as any organisational failure, or deficiency, that can be potentially caused and/or originated by a human, including, internal or external human actions or non-actions.

Despite the lack of empirical literature on people risk, McConnell (2008) has made a substantial contribution to the academic literature by proposing that, in order to understand people risk; it is essential to understand its boundaries. His argument is that, without an understanding of these boundaries, critical risks may (involuntarily) be neglected while OpRisk managers may lack the necessary skills to fully comprehend it. Thus, being unable to suggest appropriate mitigation techniques, and subsequently, being unable to calculate the relative risks comprising OpRisks, a procedure which is essential for accurate setting of the capital requirements. Therefore, in order to capture these boundaries, he

constracted a 'generic' People Risk Framework (Figure 5) with the aim of identifying and clarifying the scope of people risk. In this theoretical framework he goes beyond the hierarchical level suggested by Blunden and Thirlwell (2010), by arguing that people risks can be considered as occurring within four dinstinct, escalating areas:

1. Incident: *how do people, especially employees, react when an unforeseen 'incident", such as the processing of an incorrect transaction, occurs?*

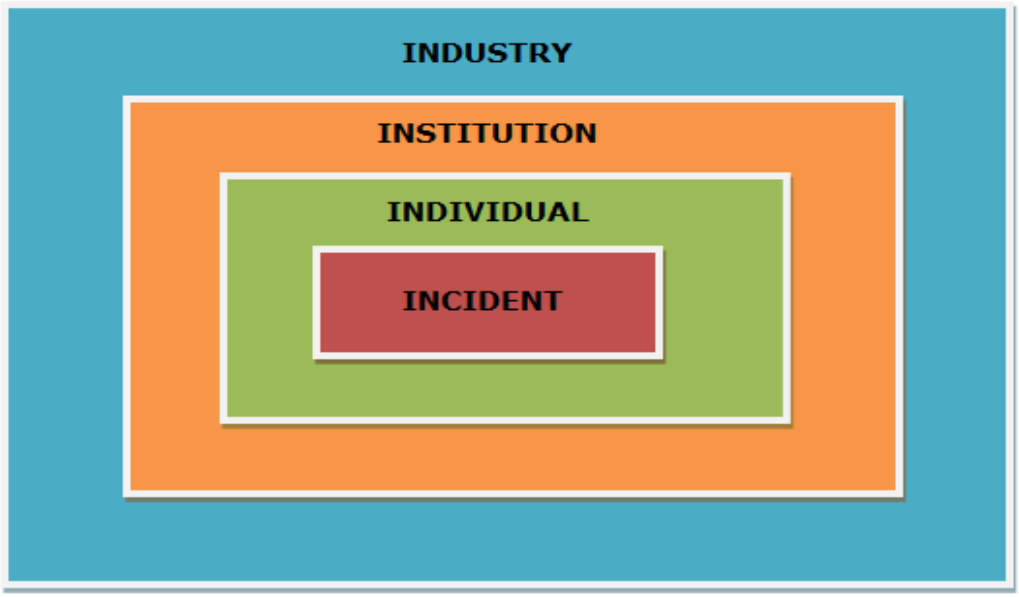
2. Individual: *how does an individual (or a small group of individuals) behave with respect to their responsibilities (such as, representations made to customers with regard to the properties of a particular financial product (i.e. mortgages)?*

3. Institution: *how does the firm behave with respect to the behaviour of the individuals whom it employs, and with whom it deals (for example, turning a blind eye to profitable, but suspect, transactions)?*

4. Industry: *how does the industry as a whole behave (for example, emulating one another in structuring and selling dangerous, potentially illegal, products and services)?*

(McConnell, 2008: p.373)

Figure 5 People Risk Framework (McConnell, 2008)



McConnell (2008) argues that when cosidering people risk and how to manage it, a key aspect is the 'intention' of the people involved. When an incident is 'unexpected', it is rarely the intention of the people, rather, it is usually a result of lack of knowledge, experience, training or plain error. At the individual and institution level, risky activities can be classified as intentional, with the people involved being aware of the consequences of their actions, or unintentional, where adverse outcomes can result from ignorance or inexperience. He then identified three types of intentional 'misbehaviour', which adverse outcomes can result from:

- Illegal: an individual intentionally breaks the law i.e. theft, insider trading, market abuse
- Unethical: unethical within the bounds of the law, but unacceptable in normal business, such as, failing to provide all information upon which to make an investment decision
- Inappropriate: unacceptable behavior such as aggressive sales techniques.

However, these types of misbehaviour can rarely be identified due to the blurred lines between them (McConnell, 2008; McConnell & Blacker, 2011; 2012).

This framework has impacted substantially the OpRisk literature, as it has introduced people risk as an emerging standalone area in this research field. In fact, following McConnell's article on people risk (People Risk: Where are the

Boundaries?, 2008) additional authors started referring to 'people risk' in their academic papers, including; (Martin, 2009; McConnell & Blacker, 2011; 2012; Bryce, et al., 2013, etc.). However, despite the immense role that the People Risk Framework has played in the empirical literature around this niche area, this framework is based on theoretical arguments, while any empirical proof about its applicability in practice is absent. Therefore, it is anticipated that this paper will capture this gap in this niche body of literature.

3. Methodology and Data Collection

3.1. Introduction

The following section will explain the method used in order to conduct the research, while it will provide a descriptive analysis of the data collection process, the sample, and the analysis technique.

3.2. Aims and Objectives

The central focus of this paper is to to test the validity of the People Risk Framework using the FSAFN as evidence, while generating new knowlegde surrounding people risk. The investigation will seek to identify human behaviour in the FSAFN and correlate it with the framework, to examine whether human activites exist under each of its constituting dimensions. In the absence of guidelines on people risk management in the financial services regulatory framework, it is anticipated that such an investigation would provide crucial insights on whether this framework can be used by firms in real life to tackle the impact of people risk in financial institutions that, may potentially be useful in setting OpRisk capital more accurately. The paper also aims to provide recommendations for future research and implications for the organisational and regulatory practice.

3.3. Method

In order to achieve the aims and objectives of this paper, a qualitative content analysis will be conducted. This method is defined as, a research method for the subjective interpretation of the content of text data through the systematic classification process of coding, and identifying themes or patterns, that contribute to the provision of knowledge and understanding of the phenomenon under study (Downe-Wamboldt, 1992; Hsieh & Shannon, 2005). Additionally, it consists of three types of approaches, however, this study will implement the direct approach, which aims to 'validate, or extend conceptually, a theoretical framework or theory' (Hsieh & Shannon, 2005). This approach is often associated with the deductive category application approach in which, relationships amongst the variables assist in determining relationships within the coding scheme (Mayring, 2000). Therefore, the study will implement a direct deductive content analysis by embedding the documented data derived from the FSAFN into the People Risk Framework.

According to Hsieh and Shannon (2005), this type of analysis follows a structured process; initially key concepts/variables are identified using the existing theory, and then, operational definitions for each category are determined using the theory. In this case, the four dimensions of the framework are going to be used to identify people's behaviour in the FSAFN. Since the data used is secondary, the process will start with 'coding' immediately with the predetermined codes, i.e. identify the data immediately under each category. The findings from such an analysis may offer supporting or non-supportive evidence for the theory. Additionally, the existing theory will guide the discussion of findings, which is the main strength of this approach, as it allows theory to be expanded or supported conveniently (Hsieh & Shannon, 2005). Its implementation has also some 'inherent limitations' in that, researchers approach the data with an informed, yet strong bias, which induces practisioners to be more likely to find supportive evidence, rather than non-supportive, of the theory. According to Lincoln and Guba (1985), these limitations are related to 'neutrality' or 'conformability of trustworthiness' as a parallel concept to objectivity.

Moreover, although this is not the first time the framework's existence is acknowledged in academic papers (see McConnell and Blacker, 2011; 2012), this

current paper will evaluate the strength of this framework. Essentially, this is the first time that the People Risk Framework is being examined in a research paper, justifying the absence of public sources related to it. Maxwell (1992) argues that the legitimacy of qualitative research is crucial and that if qualitative studies cannot consistently produce valid results, then recommendations based on these studies cannot be relied on. This is why it is important to test the validity of the framework, indicating the contribution of this study to the existing literature.

Further, although the FSAFN have been used in research previously (see Ring et al., Forthcoming; Turner, 2005), to the author's knowledge, not only it is the first time that such an investigation is conducted, but also, it is the first time that people risk is investigated in conjunction with the FSAFN. Distinctively, this particular dataset contains detailed examples of specific operational failures describing the loss event in detail, allowing relevant data to be collected effectively. It also consists of a wide-range of operational failures, allowing conclusions to be drawn from an examination of a broader range of operational loss events. This originality also signifies the contribution of this research paper.

In essence, the FSAFN are fines issued by the FSA as a result of some illegal action, organizational failure, or regulatory compliance misalignment. The FSA uses 'public censure' through the publication of the FSAFN as a 'means' by which the regulator can communicate poor behaviour to the regulatory community, while expecting an improved conduct from regulated individuals and institutions (Turner, 2005; Ring, et al., Forthcoming). This is why the FSA considers it as a more serious crime when the underlying breached Principle is related to a failure, already being known within the sector. Moreover, through the identification of regulatory breaches, the dataset enables comparison amongst the cases, thus providing a sound dataset of operational loss events, suitable in examining the effect of people risk in the UK financial institutions. Lastly, given the business sensitivity relative to their failings and the information inadequacy generally provided by market participants relative to these failings, 'the FSAFN provide richness, transparency and robustness far beyond anything else that exists currently' (Ring, et al., Forthcoming: p.11).

3.4. Source

The FSAFN were obtained from the official FSA website[6]. Unlike the data sourced from organisations themselves which are usually subjective, and exposed to biasness, this source is considered to be free from such deficiencies. Given that this is the FSA official website, and an independent body from that of the institutions themselves, it is assumed that the documented data is trustworthy, objective, unbiased, complete and of a good quality (Bowen, 2005). Yet, it is subject to questionable accuracy and liability attached to the nature of such secondary data. Nevertheless, the FSAFN follow a 'consistent and standardised format in tone, framing, and content, thus allowing for ease in compatibility and data extraction' (Ring, et al., Forthcoming: p.12). It should be also noted that, since the data gathered fall within several distinctive years, it may not accurately reflect the continuously changing regulation that is in effect today.

3.5. Sample Criteria

With the purpose of acquiring relevant and more accurate results, it was decided to examine large institutions, which their impact in the financial industry is more significant than smaller institutions. For this reason, one of the main criteria for the final notices to be included, or excluded, in the sample was for the imposed fine to amount to £1million or above, while the period of interest was the post-crisis period that is, from 1st of January 2008 to 31st of December 2012. Additionally, since the aim of the study is to examine people risk within banks and insurance firms, the cases were then filtered accordingly. With regards to the latter criterion, an institution was considered to be a bank or an insurance firm if the name of the fined institution was included either, in the list of registered banks[7], or in the list of registered insurers[8]. Where it was necessary, the Financial Services Register[9] was used, in order to accurately assess whether the institution was a bank or an insurance firm.

The only implication associated with the data selection was that some of the imposed fines were discounted, usually by 30% due to an agreement, usually of

[6] http://www.fsa.gov.uk/library/communication/notices/final
[7] http://www.fsa.gov.uk/library/other_publications/banks/2010
[8] http://www.fsa.gov.uk/consumerinformation/product_news/insurance/employers_liability/table
[9] http://www.fsa.gov.uk/register/home.do

an early settlement, resulting to an actual payment of less than £1million, i.e. original fine amounted to £1million, but the actual payment was £700,000. Hence, since the original fine was within the selection criterion, such discounted fines were included in the sample.

3.6. Data

The total number of the FSAFN that satisfied all three criteria was 34, totalling to £396,685,000 in fines. Figure 6 below depicts an upward trend of the number of these cases during the 5-year period and the total number of cases per year, while Figure 7 depicts the total amount of fines per year. The upward movement that both figures depict can be explained by the fact that the FSA had imposed stricter measures after the GFC and the run on the Northern Rock in 2007. Inevitably, these incidents have put the FSA 'under fire', since they indicated the regulatory body's failings to address deficiencies within the financial system (Allen & Overy, 2013). This phenomenon also justifies the regulatory reformation of the 'tripartite system', and the recent transformation of the FSA to FCA.

Figure 6 Number of FSAFN per year

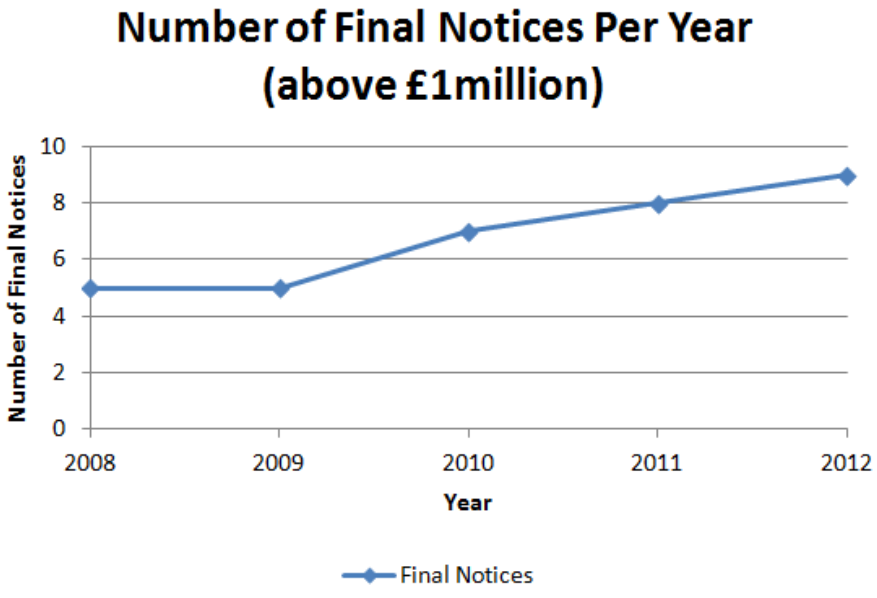
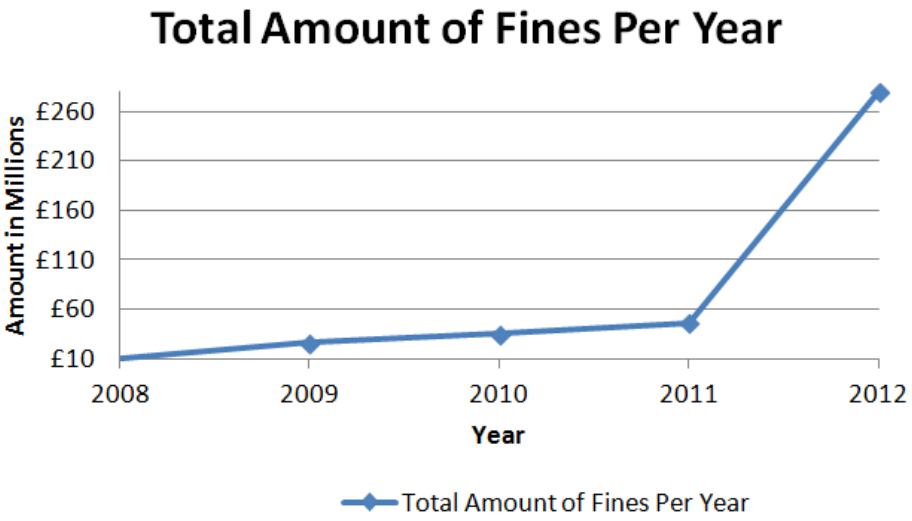


Figure 7 Total Amount of Fines per year



3.7. Descriptive Analysis

Initially, the selected cases were read in order to 'facilitate immersion in the topic' (Ring, et al. Forthcoming), while constructing a table in order to gain an insight of the cases, and the types of operational loss events. Appendix 1 briefly describes the financial losses of the institutions constituting the sample, and shows the Principle(s) breached in each case (detailed explanation of all the breaches is found in Appendix 2). The most common types of operational losses were related to 'Unfair Customer Treatment', including asset-mispricing and unsuitable advice given to customers. Rogue trading and market abuse were amongst the most serious breaches, accompanied by the most expensive financial penalties. However, the utmost serious breach was the misconduct relating to the calculation of LIBOR and EURIBOR which was conducted by UBS AG (Case 23) and Barclays Bank Plc (Case 30), amounting to £160,000,000 and £59,500,000, respectively, in fines. The cases indicated that almost all of the people-related failures were a result of corporate culture inefficiencies, which bring to the surface managerial failures regarding the implementation of a successful culture with strong internal controls to avoid intentional, or unintentional actions. Remarkably, 24 out of 34 cases involve a breach of Principle 3, which refers to breaches regarding 'Management and Control'. This analogy stresses the importance of management and internal controls within an

organisation and indicates that any inefficiencies occurring within management and control inevitably, result in operational losses. Those cases that were not involved in breaches of Principle 3, they also involved inadequate control systems and management failures (Principle 2 and 9, Appendix 2), thus indicating corporate culture failures which the senior managers and the board of directors are responsible for.

3.8. Data Collection and Analysis Technique

With the purpose of constructing a table summarising information enclosed in the FSAFN in relation to each of the dimensions in the framework, the cases were read for the second time. The goal was to identify people's actions and find correlation where possible, with the four distinctive dimensions of the framework, as indicated in Appendix 3. However, it was noted that FSAFN mostly referred to the Firm as a 'person', under Section 206 of the Act[10], with limited reference to specific individuals, such as staff, senior management, or board of directors. Therefore, the strategy implemented to collect the appropriate information for each dimension is described below:

Incident: The information sought was related to the failure on the surface of the operational loss. For example, there were instances that failure occurred from an unexpected error (i.e. system or reporting error). In other cases, failures persisted in the organisation and they were only revealed after the FSA's investigation, including unrevealed system design, and process failures. Other situations considered under 'incident' include, organisational risks rising from inadequate systems and controls.

Individual: Information related to staff behaviour was sought and it was judged whether it was intentional or unintentional. Possible reasons for employee behaviour were also recorded, for example, whether this was a result of training, supervision, or incentive schemes failure.

[10] Section 206 of the Act states: If the Authority considers that an authorised person has contravened a requirement imposed on him by, or under this Act…it may impose on him a penalty, in respect of the contravention, of such an amount as it considers appropriate.

Institution: Any information related to organisational failures and inefficiencies were reported under the category of 'institution'. Failures of management and actions of employees in the higher hierarchy were considered to be institutional losses, while any failures addressing the name of the institution were considered to be managerial losses.

Industry: The type of information that was sought was related to the impact of losses of the firm in the wider market. For example, this includes the impact on market confidence with regards to the institution's size in the industry.

Finally, with the information gathered from this process, the table in Appendix 3 was constructed, which was the main table used to conduct the analysis.

4. Findings

4.1. Introduction

Even though it was expected that one case will cover all of the four dimensions in the framework, it was indicated that not all of them satisfied all the categories (Cases: 1, 8, 11, 17, 24, 28, 29, 31, 33). It was discovered that in fact, it is very challenging to correlate the evidence with the framework, particularly, because the FSAFNs *rarely* provide description on employee actions and behaviour. In order for the data and the content analysis to be valid, consistency plays a major role. However, although the FSAFN are relatively consistent, a slight change amongst the cases across the 5 years was noticed in that, the more recent cases were more detailed than the older ones. This was also indicated by their number of pages on average; the older cases had around 15 pages whereas the newer ones had around 23 pages or above. This was an important implication in the study as the detailed descriptions allowed more relevant information to be collected, which explains why the older cases acquire less information in the table. This section will provide a discussion on findings on each of the four dimensions distinctively, followed by an evaluation of the framework as a whole.

4.2. Incident

McConnell (2008) describes that 'incident' relates to the employee actions when an 'unforeseen' incident occurs. Surprisingly, the analysis indicated that in almost all of the cases, neither employees at the operational level, nor senior staff acted, or reacted, to the 'unforeseen' incident in an efficient and appropriate manner. The analysis has also shown that failures were not always discovered or recognised by the people within the organisation. Instead, they were incubating along the organisation unnoticed. For instance; in Case 6, the rogue trader used to hide losses in his trading book amounting to $96million, which were revealed only after he became redundant. Inevitably, in such cases, no action was taken due to the ignorance of the state of events. Similarly, in Case 14, uncovered ongoing failures came into surface only after the data loss incident. Notably, in most of the cases, failures occurred as a result of undiscovered process failures usually at the operational level, rather than unexpected incidents, i.e. failures resulted from the sales process design that encouraged sales advisers to follow 'assumptive' selling techniques (Cases: 1, 3, 5), and to provide insufficient information to customers, exposing them in the risk of making decisions based on incomplete or inaccurate information (Cases: 18, 19, 20, 21, 24, 33).

Although such activities are considered inappropriate, it is expected that front row employees will not recognise them as inappropriate, since they are part of their daily activities, and it is simply how they are trained to do their job. Consequently, it is through the monitoring and supervision that these failures are expected to be revealed. In fact, as indicated in Appendix 4, the incident or the failures were recognised internally in only 10 out of the 34 cases in the sample, while only in 4 of those cases, people at the operational level escalated the information about the failures across the hierarchy (Cases: 4, 17, 20, 23). Yet, even when the information was escalated at the senior level, managers failed to take appropriate actions and mitigate failures and risks. For example, in Case 4, a system error resulted into asset mispricing, however, lack of fast information flow resulted into 'reactive' decision-making, exposing customers in the insurance market, causing further compliance failures (i.e. unfair customer treatment). Hence, revealing that, the firm's core value was not to treat customers fairly. This incident can be associated with McConnell (2008)'s

argument that losses from unexpected events (system error) rarely result from the intention of the people involved to act in a way that causes a loss, but rather, factors such as lack of knowledge, plain errors or stress of their job (managerial decision) induce them to make 'bad decisions' (indicating poorly defined culture). Alternatively, if the institution had operated in a manner that its core values and its culture are both aligned with the FSA's requirements, and if any action taken these values were taken into consideration, it would have been 'almost' impossible that such a 'reactive' decision would have been taken. Therefore, although it may be considered that false decisions usually result from operating under stress and pressure, thus they are not intentional, generally, they reveal an 'ill-defined' culture.

In support of McConnell's statement, the cases revealed that 'experience' plays a crucial role when it comes to handling of an unforeseen incident. Case 6 indicated that rogue trading losses remained unrevealed largely as a consequence of 'unexpected staff turnover' which resulted into the rise of failures derived from inexperienced staff and lack of knowledge on selling products. Case 31 provides an even stronger example of the importance of having experienced and adequate staff at crucial positions. To illustrate, during the relevant period, the institution was going through a serious business strategy restructuring which required strong managerial support, board oversight and powerful systems and controls. However, as a result of its staff rotating scheme (typically 3 years), personnel with limited experience, skills and knowledge, and most importantly, with inadequate level of understanding of the FSA requirements, were placed at senior positions, including the CEO. Unsurprisingly, the developing operations proved to be a failure as a result of poor corporate governance and control arrangements. Although this incident occurred along the senior positions, it gives a strong insight of the importance of staff experience, risk of staff turnover and rotational staff schemes in every hierarchical level.

This analysis supports that scenario analysis and learning culture play an important role in risk management, as they target at reducing uncertainties regarding employee behaviour under unexpected loss incidents, which is achieved through enhancing the level of employee experience under unforeseen events. In fact, learning culture can be used as supplementary to scenario analysis by using known events in the scenario analysis. This is also why the FSA

uses 'public censure' and warning notices as means to raise awareness within the financial industry, anticipating that managers will take the appropriate measures to eliminate particular events. Interestingly, the analysis indicated that managers failed to take such warnings seriously. To exemplify, at the senior level, 10 out of the 24 'unrecognised' incidents (Appendix 4) could have been recognised, and even avoided, if managers had taken appropriate actions after the FSA warnings regarding the specific incident. Moreover, given that these incidents had occurred in a period of increased awareness about the particular 'incident', it is unsurprising that this implication was an additional consideration when imposing the financial penalty. To justify, history has shown that rogue trading results from a common set of internal control failures, such as lack of monitoring and supervision over trading procedures. Nonetheless, the FSAFN revealed that institutions fail to take appropriate measures to mitigate such risks (Cases: 6, 12, 27), while warnings and indications submitted in public by the FSA are greatly disregarded (Cases: 3, 5, 8, 9, 13, 16, 18, 31, 32). These cases indicate that despite the FSA's attempts to encourage the implementation of learning culture, institutions fail to take appropriate considerations. Indeed, with the exception of Case 31 and 34, none of types of failures or incidents, is unique (Appendix 1).

In addition to experienced staff, McConnell (2008) states that a well-trained workforce, supported by good systems and policies potentially reduces operational losses. Indeed, lack of training and/or guidance, and inappropriate training were the causes of failure at the incident level in 17 cases in the sample (Appendix 3). For example; in Cases 3, 5 and 15, losses were initiated as a result of inappropriate training that encouraged sales advisers to follow inappropriate techniques; Cases 7 and 25 involved incomplete formal training and competency scheme; Cases 8 and 9 inadequate guidance in data handling; Cases 10 and 22 lack of training and education about bribery and corruption issues; Cases 11, 18 and 31 lack of training and guidance resulting into lack of process understanding, and Cases 20 and 24 lack of product understanding. It is in these cases that 'active support' by the HR department discussed by McConnell (2008) is crucial, since their responsibility is to mitigate/resolve understaffing and lack of training.

Further, even though training plays a particular role in mitigating the risk of operational losses, the analysis reveals that if training is not supported by

monitoring, control and supervision, then institutions are still in danger of becoming a victim of people risks. This is revealed by the fact that those incidents which had originated as a result of intentional behaviour (Cases: 6, 14, 19, 21, 22, 27, 30) in reality, they had arisen as a result of, either lack of monitoring, or supervision. In these cases, failure in organisational culture is implied, since a firm's culture dictates whether employees will follow the internal rules and procedures when their managers or supervisors are not around, and whether new employees will carry out their work in best practice, as they have received during their induction and training (Cognisco, 2013). Therefore, in support of McConnell (2008)'s argument, a working environment filled with experienced workforce and 'approachable' supervisors available to monitor and guide the employee behaviour under 'unusual' occasions, reduces the probability that small losses grow into large losses. This is because with an ongoing monitoring and supervision, minor losses are revealed and fixed at an early stage thus preventing incubation of failures; as it has happened in 24 out of the 34 cases in the sample, where failures remained unnoticed.

Furthermore, escalation of information flow across the hierarchy is particularly crucial especially at the operational level. This is because, although everything starts from there, central decisions are taken by senior members who are not on-site of these operations. This is why it is important for managers to make regular inspections and understand in-depth the work at the operational level, in order to mitigate the threat of negligence of risks existing at the front-row. For instance, Case 17 involves origination of the incident or error from an external third party at the front office. If the staff had not passed this information, managers would have been left unaware of the incident, thus making decisions based on ill-defined grounds. Case 4 also stresses the importance of passing the information in a timely manner, as it showed that although employees raised concerns on the issues, managers received delayed information, making them unable to take effective action on time. Therefore, during unexpected incidents, it is important to have proper controls in place to ensure that information travels along the hierarchy effectively, and efficiently. However, without strong leadership, and clearly defined roles and responsibilities to respond, or take action to the escalated information, these controls are useless (see Cases: 17, 18). Having strong communication procedures along with cooperation integrated

both, vertically and horizontally across the hierarchy, while avoiding business units operating in silos, play a substantial role in this situation. Of course, correct decisions are made only when quality information is submitted in a timely manner about everything that is going on from the front-row up to the highest level of the 'ladder', while successful communication can only be achieved through training and education that aim to establish common values and beliefs in line with organisational objectives.

In summary, at the incident level people's behaviour, actions and/or non-actions can be divided into two categories; namely, 'reaction' at the operational and at the managerial level. In brief, the people risks at the operational level are the consequences of people's behaviour at the managerial level. However, even though people risks play a substantial role in the occurrence of an incident, risk of failures are not rooted from people as such. Instead, they result from in-depth organisational and cultural failures which come into the surface only after the occurrence of an incident.

4.3. Individual

McConnell (2008) considers the 'intention' of the people involved, both at the level of individual or group of individuals, a key aspect in people risk. He identified 'unintentional' an action or behaviour arising as a result of some other form of risk, such as process risk, while 'intentional' behaviour is defined by three types of intentional 'misbehaviour', often challenging to distinguish between them; illegal, unethical and inappropriate. The analysis found evidence that McConnell (2008)'s discussion on people risk is one-sided, as it focuses merely on intentional employee behaviour originating from people themselves, thus avoiding to take into consideration risks rising from internal failures. In contrast, this analysis found that although intentional behaviour is not rare, in most cases, it was 'indirectly' induced or failed to be eliminated, by deficiencies in internal controls and systems in conjunction with process and systems design failures. A crucial finding of this study is that evidence of the existence of a correlation between the causes of behaviour, and the intention of the people has been found. Specifically, behaviour can be induced or controlled through training, incentive schemes, supervision and monitoring. Appendix 5 depicts that intentional behaviour is often followed by lack of monitoring and supervision, or lack of controls, which encourage exploitation of authority with actions remaining uncovered, while unintentional behaviour is associated with lack of training (including, lack of education, guidance, knowledge, skills and understanding) and misaligned incentive schemes.

Further, two additional types of behaviour were discovered, 'unintentional but inappropriate' associated with both, training, and training and monitoring, and 'unintentional but irresponsible' associated with monitoring and lack of controls. To justify, Case 8 and 9 involve lack of training and guidance regarding the importance of data security which resulted in unethical or inappropriate action. Therefore, even though McConnell (2008) supports that intentional behaviour consists of three types of intentional behaviour, these cases indicate that these types of misbehaviour, can also be associated with unintentional actions, as a result of ignorance about the significance or existence of certain rules and regulations. Consequently, if the staff are not trained or educated about important issues or procedures, then unsurprisingly inappropriate actions arise

without the staff being aware that their actions may breach legal or regulatory boundaries.

Although this study generally considers people behaviour that arises from lack of training and inappropriate incentive schemes as 'unintentional', since they dictate cultural failures, the employee behaviour engaged in Cases 2, 22 and 34 are considered to be intentional, as activities were *deliberately* pursued (Appendix 5). This study found that although, on the surface, is considered relatively easy to blame people (such as, in the rogue trading cases) about negative outcomes, after an in depth analysis, judging employee behaviour becomes challenging and a controversial issue, subject to subjectivity and variance in perceptions. Cases that raised such controversy in this research were often involved with a combination of training and monitoring, and incentive schemes and monitoring. However, this controversy highlights that managers can mitigate people risk through appropriate training and education, in conjunction with, ongoing supervision and monitoring upon their actions and performance. It also highlights that incentive schemes play a crucial role in aligning organisational and employee targets together. However, in order to eliminate intentional behaviour, managers need to identify the boundaries of these schemes to avoid misbehaviour relative to employee attempts to maximise self-interest. Yet, monitoring and action controls are essential.

Another important aspect of this study is that a successful implementation of a 'no blame' culture is considered to be a powerful incentive scheme in identifying and mitigating people risk. This is because it allows information about people-related failures to be communicated and escalated without employees being afraid of blame. For example, Case 14 involves intentional behaviour in relation to lack of reporting a data loss incident which had originated by an individual. If the individual, or its colleagues, were not afraid of 'blame', this information would have been passed to the managers, where appropriate measures would have been taken, thus avoiding further inefficiencies. Case 34 provides a pure justification of a 'no blame' culture in that, intentional behaviour originated after manager's announcement that 'disciplinary action' will be taken against specific employee failures, hence inducing employees to alter original documentation to avoid the blame. Therefore, in addition to McConnell (2008)'s argument, intentional employee behaviour is not always originated at the individual level,

rather, it is often induced through managerial actions or non-actions, implying that managers fail to take into consideration the consequences of their actions.

Moreover, the study revealed evidence of 'groupthink', particularly in relation to sales practices. For example, in Case 1 and 2, employees pursued their actions 'deliberately' as a result of 'groupthink' perception at the operational level. Additionally, even though McConnell (2008) fails to consider individual actions at the managerial level, the research revealed that such intentional behaviour exists at the senior level too (Cases: 23, 30). In fact, these cases acquired the highest financial penalties in the sample, both of which were involved with intentional behaviour conducted by individuals in conjunction with their managers. These managerial actions can be considered as 'groupthink' from the subordinates' perspective, encouraging them to continue pursuing illegal behaviour.

To sum up, people risk at the lower levels of the hierarchy can be mitigated through successful training, education, guidance and 'no blame' culture embedded in the organisational culture. Additionally, incentive schemes were proved to be one of the key tools in directing people actions towards the goals of the institution, where supervision and monitoring are essential supplements in setting the borders of these actions. However, evidence was found that largest losses result from intentional managerial behaviour, rather than deliberate actions at the lower hierarchical levels. Therefore, this is where domestic regulation comes into play by imposing behaviour controls at the senior level, such as personal fines, or other forms of regulatory restrictions.

4.4. Institution

From the 'institution' perspective, none of the cases in the sample incurred immense failures merely as a result of either an individual, or a group of individuals' actions at the operational level, whether these were intentional, or unintentional. Instead, 'incidents' provided a form of a 'trigger event' in order to bring to the surface institutional failures, and particularly, risks arising from ill-defined organisational culture, reckless employee behaviour at the advanced level of the hierarchy, or from systems and controls that were incubating in the organisation long before the 'trigger event' had occurred (i.e. loss at the incident level). Since the leaders of the organisation, and the promoters of organisational culture, are the senior managers, executives and board of directors, their actions inevitably have a bigger influence to the behaviour of the organisation than the standard employees. Consequently, it is the absence of management support for their own norms and policies, usually as a result of greedy behaviour (see Cases: 23, 26, 30), that 'legitimises' individuals in 'breaking the rules' (McConnell, 2008).

The study revealed limited evidence on greedy behaviour from the managerial perspective; on the contrary, managerial negligence was one of the most common behaviours found in the cases. At this level, the study considered managerial negligence to take action upon warnings or awareness of regulatory misalignments (Cases: 3, 5, 12, 13, 14, 16, 28, 31) or failures within the organisation (Cases: 6, 8, 9, 20, 25, 27) as the main cause in the relative failures (Appendix 6). This is because it is regarded to be a distinctive reckless behaviour, which gives rise to, or fails to mitigate, potential risks; hence bringing to the surface an ill-defined organisational culture which becomes responsible for the dysfunctionality of the institution as a whole. However, in accordance with McConnell (2008)'s consideration, reaction to these types of failures is not an easy task as it often requires holistic organisational change, including changing internal systems and controls, and organisational culture. As a solution, McConnell (2008) suggests that organisational change can be supported by HR. Nonetheless, this study suggests that preventive procedures could be implemented, such as, scenario analysis, learning and 'no blame' culture (see Section 4.2, 4.3), to eliminate the need of organisational change where possible.

An additional finding of the study is that, people-related failures at the institutional level are not always initiated or caused by the behaviours or actions of executive members (Appendix 6). This is because, on top of their personal actions and behaviours, internal systems and controls play a fundamental role in their performance as senior staff act, or behave, in accordance to the outcome of these internal systems and controls. In addition, a successful implementation of organisational culture along the whole of the institution is another requirement in keeping the focus of senior staff in line with the organisational objectives. However, corporate governance should always ensure that culture is in line with the FSA regulatory requirements to avoid compliance issues, as happened in the cases mentioned above. In general, for an organisation to operate in a healthy environment, organisational culture and system controls should be set successfully as managerial actions will be defined and driven through their outcomes, while people behaviour should be controlled through incentive schemes.

Similarly, McConnell (2008) supports that; culture is one of the root causes of the problems. Correspondingly, the root cause analysis conducted on the failures described in the FSAFN found evidence that 9 incidents resulted from poor culture (including, ineffective communication and inefficient information flow). For instance, in Case 4 and 18, managers took reactive decisions breaching the FSA requirements as a result of mismatching between organisational culture and the FSA Principles. Further, he argues that it is the 'social interactions' between people that cause problems in dysfunctional institutions in which 'individuals are usually at fault' as a result of unethical behaviour or lack of action and responsibility (McConnell, 2008: p.376). In fact, correlation with this argument was found in Case 7, where lack of responsibility resulted from poor social interactions amongst business units that operated in 'silos', and in Case 23, where insufficient information flow left the board unaware of the failures.

Finally, even though People Risk Framework and McConnell (2008)'s discussion upon it focuses on risks arising merely from the people themselves, and poor culture, this study reveals a significant amount of evidence on people risk arising as a result of poor internal systems and controls. More unambiguously, the study revealed that although culture and 'social interactions' do play a substantial role, individuals are not always at fault, in that behaviour or actions are significantly

induced by poor systems and controls which give the illusion that 'everything works fine' until an unexpected event occurs, revealing their deficiencies. Indeed, as indicated in Appendix 6, systems and controls contributed to the 'root' of the causes in 25 cases, corporate governance (i.e. people-related failures) in 19 cases, and organisational culture (including, ineffective communication and inefficient information flow) in 9 cases. Yet, it is important to note that even though all the cases are related to inefficient and inappropriate controls and culture implementation, these results are based on the *main* cause that originated people-related failures at the institutional level.

4.5. Industry

According to McConnell (2008), large operational losses can occur across the whole financial sector as a result of people's actions in various institutions, distinctively. As McConnell (2008) mentions, existing empirical literature revealed that, the largest losses tend to be 'fines levied on firms' for actions against clients and against employees, while the underlying causes of these losses are the employee actions within the organisation that 'caused the fines to be levied, i.e. people risk' (McConnell, 2008: p. 377). In addition to the fines imposed on the firms as a result of people behaviour, he argues that on the industrial level, herding behaviour and 'across-the-board failure of ethical standards in the industry' provide additional people-related failures within the whole industry. This argument relates to the evidence found in this current study. More explicitly, evidence shows that the FSA considers the size of the institution to be a significant factor when the fine is imposed. This is because institutions with leading position in the industry, such as nearly every institution consisting in the sample of the current study, reasonably, have the potential to promote herding behaviour in the industry. More explicitly, in their attempt to remain competitive in the market, smaller financial institutions pursue the actions and behaviour of the industry 'leaders'. Therefore, leading institutions should set an example for the smaller institutions by pursuing appropriate and legal policies and procedures, in accordance with the rules and regulations of the FSA.

The study revealed that the extent of the impact of people risk which arises from the 'incident' level, indeed, disembarks on the industrial level. In addition to the risk of herding, the analysis identified various other types of potential risks that impact the industry. Given the size of the institutions, the FSA claims that through their reckless actions, institutions had exposed the FSA at the risk of losing its integrity, and its ability to reduce financial crime, maintain market confidence, and protect customers. Maintaining market confidence is crucial in order for the financial services sector to remain in the market, however, in many of the cases, the industry became a victim of the distinctive institutional losses by losing market confidence. In this case, it can be said that people risk arising internally in one institution, becomes external people risk for another/others. In

addition to this, the operational losses described in the cases indicated that they impact substantially the regulation itself in that, in various occasions, it induced the FSA to undertake stricter measures in order to avoid further losses. Although this may be valuable from the regulatory perspective in terms of increasing even further financial security in the market, from the organisational perspective, it is considered a challenge, as institutions have to deal with tighter measures restricting their actions. Therefore, once more, it can be concluded that other independent institutions in the market, become victims of 'active' people risk of their competitors, hence indicating the difficulty involved in identifying and measuring the scope of risks associated with people behaviour and actions.

Finally, it is important to mention that, not all the cases enclosed evidence correlating with people risk at the industrial level (Appendix 7). However, the most serious cases in relation to risks directly impacting the financial industry, both domestically and internationally, were Cases 26 and 30; both of which were involved with misconduct relating to the calculation of LIBOR and EURIBOR. Since the impact of the operational losses involved in these two cases had the potential to have a tremendous 'collision' in the industry, it is no surprise that they acquire the two highest fines in the sample. Therefore, this stage of the analysis exposed the importance of the people operating within the financial industry to understand that, the extent of their behavioural impact extends beyond the institution in which they operate, and that it can potentially cause serious financial losses in the whole of the industry. Undeniably, this can only be achieved through the organisational culture, and through the FSA requirements.

4.6. Evaluation of the Framework

Considering the People Risk Framework as a whole, it can be said that, although not every single case enclosed information enabling correlation with all the cases consistently, overall, the FSAFNs do provide correlating evidence in the existence of people risk within the four dimensions distinctively. Hence, it can be concluded that real life evidence does exist, ensuring the validity of the theoretical framework in practice. However, the analysis revealed some critical complications suggesting a review of the framework in specific aspects. First and foremost, the explanation of the framework was found to be brief and basic, thus facing difficulties in relating the evidence with the theory consistently. This outcome was also induced due to the anticipated imperfect matching between theory and evidence. In addition, distinguishing people risk in the FSAFN was challenging not only because the descriptive analysis of the fines was mostly referring to institutions themselves, rather than individuals' activities, but also because employee actions are interrelated indicating the difficulty in separating such evidence under each dimension. This is because the evidence indicating people-related failure in each dimension does not occur in a 'silo' manner, such as the framework implies. Rather, these failures are systemic in that, one action rises after the other, resulting into an 'inseparable' chain of 'behavioural' events within all of the dimensions. Therefore, even though people risk exists within all the four dimensions, they cannot be treated separately. Hence, when organisations are considering mitigation strategies in relation to people risk, they should regard them as an integral operation.

Further, McConnell (2008) considers people risk, risks that arise from people themselves. Although this is the 'pure' meaning of people risk, the study revealed that, in most of the cases, people-related failures arise as a result of poor internal systems and controls, rather than from behaviour at an individual level. However, it should be noted that this implication was extracted based on the limited information acquired from the FSAFN concerning individual behaviour. Although these failures may be regarded as process and system risk, this study suggests that it may be regarded as an additional dimension within the framework, and particularly under 'institution', in which people risk potentially rises. Similarly, even though the cases provided limited reference to the failures

occurring within the 'Three lines of defence' model, the analysis of the cases indicated that it would be useful to integrate this approach within the framework in order to gain further insights of people risks. Additionally, another possible consideration is to include hierarchy levels in addition to the four dimensions in the framework, since intentional behaviour was recognised not only at the low level of the hierarchy, but rather across several levels. Considering these arguments, it may be suggested that the framework provides fundamental grounds in identifying potential areas of people risk; however there is room for improvements.

Moreover, throughout the study it was revealed that the framework provides a powerful tool when it comes to learning lessons and additional insights regarding the analysis of operational losses. This is because it can be used by practitioners as a guiding mechanism as to identify the scope of people risk. Therefore, it can be concluded that the People Risk Framework has the potential to become an even stronger mechanism in the emerging literature of people risk, by suggesting that a more detailed and extended version of the framework would be more useful for its practitioners.

5. Conclusion and Recommendations

The aim of the paper was to investigate the validity of the People Risk Framework, proposed by McConnell (2008) with the purpose of identifying the diverse boundaries of people risk. In particular, this study has examined the extent to which this theoretical framework is applicable in real-life by attempting to find a correlation between the theoretical dimensions comprising the framework, namely, incident, individual, institution and industry; and factual evidence, using operational loss events. Hence, evidence was sought within the FSAFN imposed to large banks and insurers operating within the UK for the last five years. By undertaking a content analysis of the sample cases, this study has shown that, correlating evidence does exists in the FSAFN, hence concluding that the framework is applicable in practise. However, the study supports that the framework is generic, providing the basic grounds for capturing people risk. The evidence from this study suggests that there are additional aspects to be considered when identifying the scope of people risk. In particular, it was identified that the main causes of the rise of people risk in the FSAFN were the result of poor internal systems and controls, especially relative to training and monitoring, and incentive schemes, giving rise to system and process risk through which people risk was then generated. This finding contradicts with the existing theory suggesting that people risk rises as a result of intentional employee behaviour. In fact, this type of behaviour was hardly recognised in the evidence.

Additionally, although a limited number of cases were referring to the 'Three lines of defence' model, the study suggests that considering this approach when dealing with people risk management may provide further useful insights. The study also suggests a possible restructuring of the framework considering people risk along the hierarchical levels, as it was revealed that risky behaviour does not only occur at the low level of the hierarchy as the framework suggests. In fact, the study showed that intentional behaviour at the institutional level imposes more severe impacts.

Moreover, it was indicated that not all the losses arise as a result of unexpected loss events. Even when considering external factors such as the GFC as an 'unexpected' incident, it was indicated that losses resulted from failures well

before the 'unexpected' event; hence, demonstrating real evidence on the need of proactive risk management, supported by Martin (2009), Ashby (2009) and, Blunden and Thirlwell (2010). McConnell (2008) suggests that it is important for operational risk managers to cooperate with the HR department in order to control and eliminate risky behaviour, through training and education, and maintain a satisfactory working environment. Yet, even when employees are well-trained, employee behaviour during the potential 'unexpected' event remains unforeseen. Despite its exploratory nature, this study offers some insight into possible learning outcomes through the investigation of the FSAFN. Particularly, one of the outcomes of this study is that, in addition to the scenario analysis and learning culture, a powerful people risk mitigating technique, is the successful implementation of a 'no blame' culture. This technique not only enables managers to gain even more insights concerning the potential areas that people risks may arise, but also it allows escalation of information concerning people-related failures without employees being afraid of losing their job. Importantly, it also allows reporting of information about small failures or 'near misses', caused by employees, that may otherwise cause serious consequences in the organisations through decision-making based on unreliable information.

Given that to the author's knowledge, the People Risk Framework is roughly the only existing literature that aims to capture the broadness of the scope of people risk, the current study contributes to existing knowledge by providing assurance on the effectiveness of this framework, allowing further studies to be built upon these grounds. Additionally, the current paper adds substantially to the level of understanding the framework, and people risk itself. It also provides a useful example for future practitioners, as to what type of evidence can be used with this framework, and how to approach it, while it provides considerations for additional developments in areas which people risks may occur. It also introduces to the research field an innovative and rich dataset (i.e. the FSAFN) which can provide crucial insights into operational risk failures.

Furthermore, although the study has reached its objectives, there are some unavoidable limitations which should be considered. Firstly, the understanding and interpretation of the underlying framework itself is based on subjectivity, and depends on individuals' perception. Since the author of the proposed framework (P. McConnell) has provided limited description and explanation of the

framework, it increases the level of variances in perception. Secondly, the study acknowledges that to generate valid results, consistency is required. However, maintaining consistency throughout the data collection and analysis of each case was challenging due to the nature of the database. Particularly, although overall the cases were consistent, slight differences still exist over the years, such as the changing regulatory environment. Notably, the fact that the study was conducted by a single researcher reduces the level of its validity. Thirdly, findings are subject to the limited availability of the relevant information enclosed in the documented data, its accuracy, and its biasness. Last but not least, the findings are limited to the small size of the sample and the short period of interest. They also represent only a small proportion of the financial services sector, as the data includes only banks and insurers operating in the UK. Therefore, caution must be applied when drawing conclusions, as the findings may not be valid in more generic terms.

Moreover, this current study reveals that a number of possible future studies using the same experimental concept are apparent. To begin with, it is recommended to repeat the same experimental dataset undertaken by more than one researcher and for a longer period of time to acquire more valid results. Additionally, it would be interesting to examine the effect of people risk before and after the financial crisis, and/or the differences between the FSA and FCA, using the underlying framework to reveal whether regulatory changes have an effective impact on the people risk mitigation. Interestingly, the study has revealed that the particular experimental concept provides potentially valuable learning outcomes concerning people risk identification and mitigation techniques. Further, since the impact of financial regulation 'disembarks' in international markets, it would be interesting to conduct a cross-national comparative study using evidence of all the domestic regulatory fines in order to allow the findings to be relevant at the international level. In relation to this, it would also be interesting to undertake the same study in order to investigate the impact of Basel III and Solvency II on people risk to identify possible regulatory improvements.

Finally, one of the most significant implications of this study is the recognition of the importance of people working within such large financial institutions, to be aware, and understand, the extent to which the impact of their actions, or

behaviour, may have. Recognising the fact that any type of misbehaviour may have a substantial impact, beyond the institution in which they function, may potentially encourage a more responsible behaviour in the employee routine operations. Therefore, an important starting point in encouraging this type of behaviour would be for the FSA, or the current FCA, to emphasise personal behaviour and actions within the final notices, rather than merely attributing the failures to the organisation in general. This is suggested in order to stress the importance of the consequences of the employee actions. Of course, this cannot be achieved without the help of embedding this attribute in the organisational culture, which can be further reimbursed by adding such a requirement in the regulatory framework. In addition to the disclosure of specific employee actions, the FSA could impose stricter measures towards managerial behaviour, such as personal fines or restrictions, in order to indicate the importance of their roles and responsibilities and also to limit intentional behaviour at the senior level. Further, since the senior level performance depends on the outcomes of internal systems and controls, and with the FSA being responsible to control this performance; the FSA could impose regular assessments on these controls to ensure that seniors perform based on 'healthy' grounds.

In conclusion, although there is a lack of literature in people risk, nevertheless, it does not cease to elevate its value; and the applicability of using the People Risk Framework in real life is further reinforced by this research, acting as a stepping stone to the emerging literature.

6. References

Al-Darwish, A., Hafeman, M., Impavido, G., Kemp, M., & O'Malley, P. (2011). Possible unintended consequences of Basel III and Solvency II. *International Monetary Fund 11*(187).

Allen & Overy. (2013). *The Fiancial Conduct Authority - An Overview.* Allen & Overy LLP.

Ashby, S. (2008, May 16). Operational Risk: Lessons from non-financial organisations. *Journal of Risk Management in Fiancial Institutions, 1*(4): pp. 406-415.

Ashby, S. (2009). *The Turner Review on the Global Banking Crisis: A Response from the Financial Services Research Forum.*

Ashby, S. (2010). *The 2007-09 Financial Crisis: Learning the Risk Management Lessons.* Nottingham: Financial Services Research Forum.

Association of British Insurers (ABI). (2011). UK Insurance Key Facts. London: ABI: Association of British Insurers.

Association of Independent Financial Advisers (AIFA). (2012). *Consumer Trust in Financial Services.* London: Association of Independent Financial Advisers.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation.* Oxford: Oxford University Press.

Bank for International Settlements (BIS). (2011). *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches.* Basel Committee on Banking Supervision, SIG Operational Risk Subgroup. Switzerland: Bank for International Settlements.

Basel Committee on Banking Supervision (BCBS). (2006, June). International Convergence of Capital Measurement and Capital Standards. A Revised Framework. *Comprehensive Version*.

Blunden, T. (2003). Scoreboard Approaches. In C. Alexander (Ed.), *Operational Risk: Regulation, Analysis and Managememnt* (pp. 229-240). London: Prentice Hall - Financial Times.

Blunden, T., & Thirlwell, J. (2010). People Risk. In *Mastering Operational Risk* (pp. 269-285). London: Prentice Hall - Financial Times.

Bowen, G. (2005, June). Preparing a Qualitative Research-Based Dissertation: Lessons Learned. *The Qualitative Report Volume, 10*(2): pp. 208-222.

British Bankers Association (BBA). (2012). BBA Abstract of Banking Statistics. *29.* London BBA: British Bankers Association.

Bryce, C., Cheevers, C., & Webb, R. (2013). Operational Risk Escalation: An Empirical Analysis of UK Call Centres. *International Review of Financial Analysis*.

Bryce, C., Ring, P. J., Clark, G., Cheever, C., & Webb, R. (Forthcoming). Strategic Lessons from Banking Compliance? The importance of risk escalation for Solvency II Implementation.

Bryce, C., Webb, R., & Adams, J. (2011). Internal Loss Data Collection Implementation: Evidence from a large UK financial institution. *Journal of Risk Research, 14*(10): pp. 1161-1176.

Buchelt, R., & Unteregger, S. (2004). *Cultural Risk and Risk Culture: Operational Risk after Basel II.* Financial Stability Report.

Cetina, K. K., & Preda, A. (2005). *The Sociology of Financial Markets.* New York: Oxford University Press Inc.

Cihák, M., Demirguç-Kunt, A., & Johnston, R. (2013). Incentive Audits: A New Approach to Financial Regulation. World Bank Policy Research Working Paper No. 6308.

Cognisco. (2013). *Cultural & Human Factors in Identifying and Reducing People Risk.* Retrieved September 6, 2013, from http://www.cognisco.com/cultural-human-factors-in-identifying-and-reducing-people-risk/?goback=.gde_4929356_member_251662844

Cummins, D., Lewis, C., & Wei, R. (2006). The market value impact of operational loss events for US banks and insurers. *Journal of Banking and Finance, 30*(10): pp. 2605-2634.

Dedu, V., Turcan, C., & Turcan, R. (2011). A Behavioral Approach To The Global Financial Crisis. *The Annals of the University of Oradea. Economic Sciences., 1*: pp. 340-346.

Dowd, K. (2006, September-October). The Invisible Problem of Risk Blindness. *Financial Engineering News*(51): pp. 27-34.

Downe-Wamboldt, B. (1992). Content analysis: Method, applications, and issues. *Health Care forWomen International, 13*: pp. 313-321.

Falkner, R., & Gerty, J. (2006). A Summary of the Financial Services Authority's Enforcement Procedures in the United Kingdom. *Journal of Investment Compliance, 7*(1): pp. 69-82.

Financial Conduct Authority (FCA). (2013). *The Financial Services Register*. Retrieved August 5, 2013, from http://www.fsa.gov.uk/register/home.do

Financial Services Authority (FSA). (2010, September 9). *Goldman Sachs International.* Retrieved July 29, 2013, from www.fca.org.uk/static/pubs/final/goldman_sachs_int.pdf

Financial Services Authority (FSA). (2011a). *FSA fines Barclays 7.7 million for investment advice failings and secures as much as 60 million in redress for customers.* London: Financial Services Authority.

Financial Services Authority (FSA). (2011b). *Enhancing Frameworks in the Standardised Approach to Operational Risk - Guidance Note.* Financial Services Authority.

Financial Services Authority (FSA). (2013a). *Final notices*. Retrieved June 30, 2013, from http://www.fsa.gov.uk/library/communication/notices/final

Financial Services Authority (FSA). (2013b). *List of banks*. Retrieved August 5, 2013, from http://www.fsa.gov.uk/library/other_publications/banks

Financial Services Authority (FSA). (2013c). *List of Insurers*. Retrieved August 5, 2013, from http://www.fsa.gov.uk/consumerinformation/product_news/insurance/employers_liability/table

Gatzert, N., & Wesker, H. (2011). A Comparative Assessment of Basel II/III and Solvency II. Nuremberg, Germany: Friedrich-Alexander-University of Erlangen-Nuremberg.

Goldstein, M., & Véron, N. (2011). Too Big to Fail: The Transatlantic Debate. Washington, DC: Peterson Institute for International Economics Working Paper 11-2, PIIE.

Gov.UK. (2011). *Deputy Prime Minister's speech to MEDEF.* London: Gov.UK.

Hoyte, P. (2005). Banking on Regulatory Change. *CMA Management , 79*(4): pp. 4-30.

Hsieh, H., & Shannon, S. (2005, November). Three Approaches to Qualitative Content Analysis. *Qual Health Res, 15*: pp. 1277-1288.

Institute of International Finance (IIF). (2008). *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations.* Institute of International Finance. Washington DC: Institute of International Finance.

International Institute of Finance (IIF). (2009). *Reform in the Financial Services Industry: Strengthening Practices for a More Stable Industry.* International Institute of Finance.

Kirkpatrick, G. (2009). The Corporate Governance Lessons from the Financial Crisis. *Financial Market Trends, 2009/1*.

Levy, C., Lamarre, E., & Twining, J. (2010, February). Taking Control of Organisational Risk Culture. *McKinsey Working Papers on Risk*(16).

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Beverly Hills, CA: Sage.

Lloyds. (2013). *Solvency II implementation date*. Retrieved September 11, 2013, from http://www.lloyds.com/the-market/operating-at-lloyds/solvency-ii/legislative-developments/solvency-ii-implementation-date

Martin, P. (2009). As Risk Management Evolves, Is Operational Risk Management Important? *Journal of Operational Risk, 4*(4): pp. 75-84.

Maxwell, J. (1992, Fall). Understanding and Validity in Qualitative Research. *Harvard Educational Review, 62*(3): pp. 279-300.

Mayring, P. (2000). Qualitative Content Analysis. *Forum: Qualitative Social Research, 1*(2): pp.1-9.

McConnell, P. (2008). People Risk: Where are the boundaries? *Journal of Risk Management in Financial Institutions, 1*(4): pp. 370-381.

McConnell, P., & Blacker, K. (2011, Fall). The role of systemic people risk in the global financial crisis. *The Journal of Operational Risk, 6*(3): pp. 65-123.

McConnell, P., & Blacker, K. (2012, Spring). Systemic Operational Risk: the UK PPI Scandal. *The Journal of Operational Risk, 7*(1): pp. 79-139.

Meyer, L. (2000, August 31). Why risk management is important for global financial institutions. *Central Bank Articles and Speeches*.

Moeller, R. (2007). *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Montross, T. (2011). Solvency II. (K. M., Ed.) *Risk Management Review*: pp. 1-3.

Moosa, I. (2007). Operational risk: A Survey. *Financial Markets, Institutions & Instruments, 16*: pp. 167–200.

Moran, M. (1989). *The politics of the financial services industry.* London: Macmillan.

OECD. (2004). *OECD Principles of Corporate Governance* (2nd ed.). Paris: OECD Publications.

Oesterreichische Nationalbank & Austrian Financial Market Authority (OeNB & FMA). (2006). *Guidelines on Operational Risk Management.* Vienna: Oesterreichische Nationalbank (OeNB); Austrian Financial Market Authority (FMA).

Ötker-Robe, İ., Narain, A., Ilyina, A., & Surti, J. (2011). The Too-Important-to-Fail Conundrum: Impossible to Ignore and Difficult to Resolve. IMF Staff Discussion Note SDN/11/12.

Patton, M. Q. (2002). *Qualitative Research and Evaluation Methods.* Thousand Oaks, CA: Sage.

Power, M. (2003). *The Invention of Operational Risk.* London School of Economics and Political Sciences. London: Centre of Analysis of Risk and Regulation.

Power, M. (2005). The invention of Operation Risk. *Review of International Political Economy, 12*(4): pp. 577-599.

Power, M. (2012). The apparatus of fraud risk. *Accounting, Organisations and Society*.

Rajan, R. (2010). *Fault Lines: How hidden Fractures Still Threaten the World Economy.* Princeton: Princeton University Press.

Reuters. (2011, May 9). *Update 6 - Trio of British Banks that $3 bln mis-selling hit.* Retrieved August 20, 2013, from Reuters UK: http://uk.reuters.com/article/2011/05/09/britain-banks-idUKLDE74805E20110509

Ring, P., Bryce, C., McKinney, R., & Webb, R. (Forthcoming). *Taking Notice of Risk Culture - The Regulator's Approach.*

Schooner, H., & Taylor, M. (2010). The Regulation After the Financial Crisis. In *Global Banking Regulation*: pp. 279-295.

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization , 85:* pp. 191– 206.

Sutton, C., & Jenkins, B. (2007). *The Role of Financial Services Sector in Expanding Economic Opportunity.* Kennedy School of Governance, Harvard University, Corporate Social Responsibility Report, Cambridge.

Teeters, N. (1983). The Role Of Banks In The International Financial System Federal Reserve System,. *Journal Of Banking And Finance , 7*: pp. 453-463.

The Geneva Association. (2010). *Systemic Risk in Insurance. An analysis of insurance and financial stability.* Risk & Insurance Economics. The Geneva Association Systemic Risk Working Group.

The Institute of Operational Risk (IOR). (2010). *Operational Risk Governance.* Sound Practice Guidance. The Institute of Operational Risk.

TheCityUK. (2012). *Key Facts About UK Financial and Professional Services.* London: TheCityUK.

Treanor, J. (2013, August 20). Barclays Branch Chief Vows Culture Change at Scandal-hit Bank. *The Guardian*: pp. 1-3.

Tuckett, D. (2009). Addressing the Psychology of Financial Markets. *Open Assessment E-Journal, 3*: pp. 2009-2040.

Turner, B. (1976). The organisational and Interorganisational Develoipment of Disasters. *Administrative Science Quarterly, 21*: pp. 387-397.

Turner, B. (1978). *Manmade Disasters.* London: Wykenham Press.

Turner, B. (1991, April 1). The Development of a Safety Culture. *Chemistry and Industry*: pp. 241-243.

Turner, B. A. (1994). Causes of Disaster: Sloppy Management. *British Journal of Management, 5*(3): pp. 25-219.

Turner, R. (2005). The interaction between FSA Enforcement Action and compliance culture: a help or a hindrance? *Journal of Financial Regulation and Compliance, 13*(2): pp. 142-145.

Watkins, S. (2013, April 17). *Rogue Traders.* Retrieved August 18, 2013, from CIMA: http://www.fm-magazine.com/feature/depth/rogue-traders

World Bank. (2012). *Global Financial Development Report 2013: Rethinking the Role of the State in Finance.* Washington, DC: World Bank.

7. Appendices

Appendix 1: Brief Description of the Final Notices in the sample

Year	Case	Institution Name	Brief Description	Principles Breached	Penalty
2008	1	Eggs Banking Plc	Unfair Customer Treatment: non-advised telephone sales of credit card payment protection insurance (PPI)	3, 6	£1,030,000
2008	2	Credit Suisse International and Credit Suisse Securities (EU) Ltd	Mispricing of Asset-backed securities by a small number of traders	3, 2	£5,600,000
2008	3	Liverpool Victoria Banking Services Limited	Unfair Customer Treatment: sales of payment protection insurance (PPI) offered in connection with unsecured personal loans	3, 6, 7	£1,200,000
2008	4	Hastings Insurance Services Limited	Asset mispricing resulting to unfair customer treatment	6	£1,050,000
2008	5	HFC Bank Limited	Unfair Customer Treatment (PPI): unsuitable customer advice	3, 9	£1,085,000
2009	6	Toronto Dominion Bank (London Branch)	Rogue Trading: loss of CAD$96m into trader's book revealed after his redundancy. Failings in the systems and controls concerning trading book pricing and marking within the Credit Products Group ("CPG") business	3, 2	£10,000,000
2009	7	UBS AG	Money-Laundering-Rogue Trading: employees on the international wealth management business desk involved in unauthorised foreign exchange and precious metals trading across 39 customer accounts	3, 2	£8,000,000
2009	8	HSBC Insurance Brokers Ltd	Data Security	3	£1,000,000
2009	9	HSBC Life UK	Data Security	3	£1,610,000
2009	10	Aon Ltd	Suspicious payments to Overseas 3rd Parties of approx. US$2.5M and €3.4M	3	£5,250,000
2010	11	DB UK Bank	Unfair Customer Treatment	3, 6	£1,200,000
2010	12	Goldman Sachs International	Rogue Trading: serious violations of US securities law	2, 3, 11	£17,500,000
2010	13	Société Générale	Inaccurate, Incomplete transaction reporting	Sup17	£1,575,000
2010	14	Zurich Insurance Plc, UK branch	Data Security in outsourcing arrangements between Zurich UK and Zurich Insurance Company South Africa Ltd exposing customers to the risk of financial loss, burglary and identity theft	3, SYSC 3.1.1R, SYSC 3.2.6R	£2,275,000
2010	15	The Royal Bank of Scotland Plc, National Westminster Bank Plc, Ulster Bank Ltd, Coutts & Company	Money Laundering	20 (1)	£8,000,000
2010	16	Credit Suisse	Inaccurate and Incomplete transaction reporting	Sup17	£1,750,000

2010	17	Standard Life Assurance Ltd	Unfair Customer Treatment	3, 7	£2,450,000
2011	18	Combined Insurance Company of America	Unfair Customer Treatment	3, 6	£2,800,000
2011	19	HSBC Bank Plc, NHFA Ltd (subsidiary)	Unfair Customer Treatment	9	£10,500,000
2011	20	Coutts & Company	Unfair Customer Treatment	9	£6,300,000
2011	21	Credit Suisse	Unfair Customer Treatment	3	£5,950,000
2011	22	Willis Ltd	Risk of Bribery and Corruption	3, SYSC 3.2.6R	£6,895,000
2011	23	Bank of Scotland Plc	Aggressive Growth Strategy, with a specific focus on high-risk, sub-investment grade lending	3	£3,500,000
2011	24	Barclays Bank Plc	Unfair Customer Treatment: customers inappropriately advised	9	£7,700,000
2011	25	Royal Bank of Scotland Plc	Unfair Customer Treatment	3, 6	£2,800,000
2012	26	UBS AG	LIBOR and EURIBOR abuse, undermining the integrity of those benchmark references	3, 5	£160,000,000
2012	27	UBS AG	Rogue Trader	3, 2	£29,700,000
2012	28	Card Protection Plan Ltd	Unfair Customer Treatment: Mis- selling products for over 6-years	3, 6 , 7	£10,500,000
2012	29	Bank of Scotland plc	Mortgage Systems relied upon incorrect records for 8 years resulting into its customers not receiving important information thus making insufficiently informed decisions about their mortgage accounts	3	£4,200,000
2012	30	Barclays Bank Plc	LIBOR and EURIBOR abuse: Misconduct relative to submission rates relative to LIBOR EURIBOR setting process for 5 yrs	3, 2, 5	£59,500,000
2012	31	Mitsui Sumitomo Insurance Company (Europe) Ltd (MSIEu)	Corporate governance and control arrangements failures resulting in poor organisation and management across the whole business, following a decision to expand and diversify into a new business area	3	£3,345,000
2012	32	Coutts & Company	Money Laundering	3, SYSC	£8,750,000
2012	33	SANTANDER UK	Risk of Mis-selling products	2, 7, Rule 6.1.16	£1,500,000
2012	34	UK Insurance Ltd	Employee submit altered documentation	2	£2,170,000

Appendix 2: Description of the Principles Breached

Principle	FSA Handbook	Description
2	Skill, care and diligence	A firm must conduct its business with due skill, care and diligence.
3	Management and Control	A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
5	Market Conduct	A firm must observe proper standards of market conduct.
6	Customer's Interests	A firm must pay due regard to the interests of its customers and treat them fairly.
7	Communications with clients	A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.
9	Customers: relationships of trust	A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment.
11	Relations with Regulators	A firm must deal with its regulators in an open and cooperative way, and must disclose to the FSA appropriately anything relating to the firm of which the FSA would reasonably expect notice.
Chapter17 (SUP17)	Transaction Reporting	
SYSC 3.1.1R	Senior Management Arrangements, Systems and Controls sourcebook	A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business.
SYSC 3.2.6R	Senior Management Arrangements, Systems and Controls sourcebook	A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.
20 (1)		A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to: (a) customer due diligence measures and ongoing monitoring; (d) internal control; (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures in order to prevent activities related to money laundering and terrorist financing.
Rule 6.1.16		(1) A firm carrying on MiFID business must make available to a client, who has used or intends to use those services, information necessary for the identification of the compensation scheme or any other investor-compensation scheme of which the firm is a 22 member (including, if relevant, membership through a branch) or any alternative arrangement provided for in accordance with the Investor Compensation Directive. (2) The information under (1) must include the amount and scope of the cover offered by the compensation scheme and any rules laid down by the EEA State pursuant to article 2 (3) of the Investor Compensation Directive. (3) A firm must provide, on the client's request, information concerning the conditions governing compensation and the formalities which must be completed to obtain compensation. (4) The information provided for in this rule must be made available in a durable medium or via a website if the website conditions are satisfied in the official language or languages of the EEA State.

Appendix 3: Analysis of the Data- Evidence on the four Dimensions

Case	Brief Description	Incident	Individual	Institution (Principles breached)	Industry	Causes
1	Unfair Customer Treatment: non-advised telephone sales of credit card payment protection insurance (PPI)	Failure in system process, process risk	Unintentional, systems-think, lack of proper training	(3, 6) - Serious or systemic weakness of the management systems or internal controls		Training
2	Mis-prising of Asset-backed securities by a small number of traders	Remuneration incentives failure	Intentional misconduct, groupthink. Certain traders were able to circumvent controls by exploiting their technical knowledge and their expertise relative to certain control personnel. The pricing of the securities have a direct effect on the calculation of their personal remuneration	(3, 2) - Inefficient preventive and detective controls, absence of close supervision, failure in translating important information into actions, failures in design, implementation, operation and management of controls. Complex structures with multiple reporting lines led to uncertainty as to supervisory responsibilities. Too much reliance on inexperience and/or junior personnel. Insufficient senior level oversight was committed to supervising and supporting day-to-day processes	In its Investment Banking division, Credit Suisse has approximately 20,600 employees operating in 57 locations across 26 countries	Remuneration schemes
3	Unfair Customer Treatment: sales of payment protection insurance (PPI) offered in connection with unsecured personal loans	Sales Process Design Failure: sales process followed 'assumptive' selling technique, in which PPI was automatically included when customers asked for quotations for personal loans	Unintentional, Sales Advisers: trained to follow assumptive technique, bonus schemes attached to the PPI sales rather than sale of loan. Sales Supervisors' commission was based on PPI creating a conflict of interest with the supervision of sales staff	(3, 6, 7) - Failure of the board of directors to redesign the sales process even after the notice from the FSA to ensure that the PPI process complies with the FSA requirements	FSA will now seek to impose higher fines for firms in the PPI market where standards fall below required levels.	Training

4	Asset mispricing resulting to unfair customer treatment	System Errors which resulted in providing inaccurate insurance quotations and make unfair decisions for customers	Unintentional	(6) - Slow information flow along the hierarchy, Senior Management decision making indicated that the organisation had an ill-defined corporate culture in that its core values was not the fair treatment of the customer. Senior Management failed to inform FSA prior to its decision making. Hastings' consideration of the costs of rectifying its errors was reactive rather than proactive.	Senior management at firms had failed to take sufficiently seriously the need to address TCF risks in their business. Actions could potentially affect the confidence in the financial system and the protection of the customers. Its decision to cancel the policies means that customers will have in their records that they have an insurance cancelled despite the cancellation being through the insurer.	System Error, Slow information flow
5	Unfair Customer Treatment (PPI): unsuitable advice was given to the customers	Process Failure: Assumptive technique was followed. Staff not trained in gathering sufficient information about the customers prior to advising them. Failures resulted into unacceptable risk of unsuitable sales and a failure to treat customers fairly.	Unintentional - lack of proper training, monitoring, incentive schemes wrongly implemented	(3, 9) - Inadequate and ineffective training, compliance monitoring procedures, manager oversight and record keeping. Information flow along the hierarchy failures. Senior managers failed to ensure their PPI sales processes were meeting FSA requirements despite FSA's notifications. Management Information.	-	Training, Incentive Schemes

6	Rogue Trading: loss of CAD$96m loss into the trader's book which was revealed after his redundancy. Failings in the systems and controls concerning trading book pricing and marking within the Credit Products Group (CPG) business	Unexpected staff turnover, which resulted into lack of product knowledge and inexperienced back-office staff as a result of training	Unethical illegal behaviour of a Trader trying to hide significant losses in his trading book	(2, 3) - Failures in trader supervision and internal audit process, lack of formal review, unclear segregation of roles and responsibilities, inappropriate management reporting and disclosure issues, inadequate product knowledge or experience of back office staff. Inefficient use of existing systems and controls over what was a complex business dealing in sophisticated and often illiquid financial products to detect and prevent illegal actions. Failed in using existing systems and controls. Information flow failures as a result of poor communication which could have led to earlier detection of the pricing issues. Result: failed to price certain positions held by the Trader accurately and failed to prevent or detect these pricing issues in a timely manner. Corporate governance failure since this was not the first time that a trader caused losses as a result of mispricing issues.	Risk that market confidence would be damaged by the sudden and unexpected write-down and revaluation of securities	Training, Supervision, Lack of controls

7	Money-Laundering and Rogue Trading: certain employees on one desk in the international wealth management business had been involved in unauthorised foreign exchange and precious metals trading across 39 customer accounts	'Training and Competency' scheme was incomplete, and failed to cover all the required business areas; no formal, documented Training and Competency scheme for the Back Office	Rogue Trading - Intentional Illegal behaviour, the desk had significant autonomy and authority	(3, 2) - Inadequately managed and controlled key risks, inappropriate supervision, insufficient management information to assess the effectiveness of risk mitigation controls, inadequate management business systems and controls, much autonomy and authority was given to the Desk Heads, lack of preventative controls, ineffective reaction to the failures, business model based on honesty and supervisory obligations but not on incompetent and dishonest actions, lack of clear leadership roles and responsibilities at the front office, back-office was operating in silo, retained email facility offered to clients disabled errors or fraud detection. Absent defined and documented set of procedures-culture management information focused more on financial performance rather than risk management, compliance or training and competence staff, compliance and internal audit issues, due regard to wandering signs which could induce senior management to consider whether systems and controls are appropriate	-	Training

8	Data Security	Risk of Data Loss - staff sent unencrypted customer data to third parties, staff left data unprotected in the firm's offices even though access to the firm's offices was securely restricted, on one occasion, staff did not adequately check if they had received customer data which appeared to have been sent to the firm by a third party.	Unintentional behaviour but inappropriate as a result of inadequate guidance on how staff should handle or transfer customer data securely out of the firm, encryption of customer data sent externally was not mentioned in the guidelines booklet	(3) - Lack of relevant processes, procedures and training, lack of maintenance and establishment of effective systems and controls to manage the risks relating to data security, internal fraud or theft, specifically the risk that customer information might be lost or stolen. Inadequate assessment of the risks relating to data security, inadequate controls to manage such risks, inadequate and ineffective procedures, guidance, training and monitoring to address these risks, corporate governance failed to take the appropriate measures in relation to data security even after the FSA's advice, firm's written procedures were fragmented and not readily accessible to staff and failed to give adequate guidance on how staff should handle or transfer customer data securely. Whilst staff members were expected to report data loss to their line manager, there was no defined response plan in place for reporting such incidents	The FSA considers the fact that the control failures resulted in the loss of customer data is an aggravating feature of this case, but this is not the sole reason for imposing a penalty. The defects in the procedures alone are a cause of significant concern and routinely exposed customers to the risk of financial crime.	Inadequate guidance

9	Data Security	Risk of Data Loss - staff sent unencrypted customer data to third parties, staff left data unprotected in the firm's offices even though access to the firm's offices was securely restricted, on one occasion, staff did not adequately check if they had received customer data which appeared to have been sent to the firm by a third party.	Unintentional behaviour but inappropriate, as a result of inadequate guidance on how staff should handle or transfer customer data securely out of the firm, encryption of customer data sent externally was not mentioned in the guidelines booklet	(3) - Lack of relevant processes, procedures and training, lack of maintenance and establishment of effective systems and controls to manage the risks relating to data security, internal fraud or theft, specifically the risk that customer information might be lost or stolen, inadequate assessment of the risks relating to data security, inadequate controls to manage such risks, inadequate and ineffective procedures, guidance, training and monitoring to address these risks, corporate governance failed to take the appropriate measures in relation to data security even after the FSA's advice, firm's written procedures were fragmented and not readily accessible to staff and failed to give adequate guidance on how staff should handle or transfer customer data securely. Whilst staff members were expected to report data loss to their line manager, there was no defined response plan in place for reporting such incidents	The FSA considers the fact that the control failures resulted in the loss of customer data is an aggravating feature of this case, but this is not the sole reason for imposing a penalty. The defects in the procedures alone are a cause of significant concern and routinely exposed customers to the risk of financial crime.	Inadequate guidance

10	Suspicious payments to a number of Overseas Third Parties amounting to approximately US$2.5 million and €3.4 million during the Relevant Period.	Authorisation Process failure: Risk of bribery and corruption with making payments to non-FSA authorised overseas	Unintentional but inappropriate action: staff involved in the making of potentially inappropriate payments, lack of training and education	(3) - Failure to assess the risks in its overseas transactions, ineffective controls to mitigate risk, fail to review and monitor relationship with overseas parties in respect of specific bribery risks, lack of training and education on bribery risks, lack of routinely assessing whether bribery and corruption risks were being managed effectively, weak control environment, inadequate systems and procedures in place to prevent the matters from occurring or to discover them when they did occur, defective procedures for the authorisation of payments, inadequate checks carried out by those signing the authorisation forms, the authorisation process was deficient as it require inadequate levels of due diligence to be carried out before a relationship with an overseas party could be approved, failures in risk monitoring and management information, systems and controls failings existed in a number of major business units and for a period of nearly three years	Involvement of UK financial institutions in (potentially) corrupt practices undermines the integrity of the UK financial services sector. Unless they have in place robust systems and controls which govern the circumstances in which payments may be made to third parties, UK financial services firms risk contravening UK and/or overseas anti-bribery laws. The FSA's financial crime and market confidence statutory objectives are both endangered by UK firms' failures in this regard. Aon Ltd is one of the largest insurance and reinsurance brokerage and risk management firms in the UK and it has a leading competitive position in the market and the firm's practices set an example which is seen by other market practitioners and customers	Training
11	Unfair Customer Treatment	Process Failure: Underwriting staff had not treated all customers fairly when considering their applications for mortgages and some of them were put in risk of financial loss inconsistent approach applied on charging fees to borrowers	Unintentional: mortgage servicing staff had inadequate understanding of TCF and its implementation	(3, 6) - Lack of supervision and oversight, lack of compliance checks, inadequate systems and controls to control and organise the process effectively, lending policy was insufficient and irresponsible which created significant risk of customers being treated unfairly,	-	Training Lack of product knowledge

12	Rogue Trading: serious violations of US securities law	Illegal Transaction: GSC and Mr Tourree committed serious violations of US securities law by making misleading statements and omissions in connection with the Abacus transaction	Intentional illegal action	(2, 3, 11) - Failure to comply its UK regulatory reporting obligations to the FSA, inadequate policies, procedures, systems and controls in relation to internal communications between UK and US operations of the GS Group, senior managers were aware of certain aspects of the incident but none of them informed FSA	Goldman Sachs is a highly sophisticated firm and among the world's premier financial institutions. The firm itself and its legal and compliance functions are integrated on a global basis and the senior management of those functions are (or ought to be) in constant communication with each other regarding legal and regulatory matters across the multiple jurisdictions in which Goldman Sachs operates its global business.	Communication
13	Inaccurate and Incomplete transaction reporting	Reporting Transaction Process: failing to submit accurate transaction reports in respect of approximately 18.8 million transactions, representing 80% of its reportable transactions	Unintentional on the lower level of hierarchy	(Sup 17) - Despite an earlier acknowledgement within the Firm of the need to conduct a review of its transaction reporting regime, the Firm's inaction prevented it from performing the necessary tests and reporting the results to the FSA, SocGen's failures occurred during a period of heightened awareness around transaction reporting issue but the senior management failed to take any action	These failings endured and their impact on the FSA's ability to detect potential market abuse and reduce financial crime. As the errors also create a serious risk of hampering other competent authorities' work in maintaining market confidence	Inaccurate Reporting, Managerial Negligence

14	Data Security in the context of outsourcing arrangements (between Zurich UK and Zurich Insurance Company South Africa Limited (ZICSA)) exposing customers to the risk of financial loss, burglary and identity theft	Process Failure: ZISCA engaged a subcontractor to collect and deliver unencrypted data and to provide storage facility. Then the subcontractor itself subcontracted the collection and delivery of this data to a 3rd party contractor (unknown to ZICSA and without Zurich UK (GI)'s consent). Failings arisen after a data loss incident: subcontractors lost an unencrypted back-up tape during a routine transfer to a data storage centre. Zurich UK became aware of the incident a year later as a result of internal audit.	Unintentional: Data loss incident was not reported until a year later, raised further issues within the business, ZICSA conducted procedures without the consent of Zurich UK	(3, SYSC 3.1.1R, SYSC 3.2.6R) - Lack of ongoing risk assessment and effective monitoring over outsourcing arrangements. Lack of oversight of ZICSA may have contributed to data loss, inadequate due diligence on the data security, insufficient reporting and management information flow which prevent governance to identify, measure, manage and control data security and financial crime risks, routine monitoring was limited to regular service management conference calls, various members of senior management had responsibility for data security issues, but there was no single data security manager with overall responsibility, the failures occurred following a period of heightened awareness of financial crime issues as a result of government initiatives and increasing media coverage, unclear management responsibilities and reporting lines, lack of training and awareness regarding the understanding of data security	The cumulative impact of the failings represented a material risk to the FSA's objectives of reducing financial crime and protecting customers.	Supervision
15	Risk of Money Laundering	Absent of screening procedure related to international trade transactions, insufficient customer information was recorded	Unintentional due to lack of appropriate training and management expertise relating to UK sanctions screening	(20(1)) - inadequate screening of relevant customers and payments against the Treasury list, after screening procedure implementation failed to ensure its design and review and monitor the process, discovery and escalation of information issues,	The involvement of UK financial institutions in providing funds, economic resources or financial services to designated persons on the Treasury list undermines the UK financial services sector integrity. Unless they have in place robust systems and controls, UK financial institutions risk being used to facilitate transactions involving sanctions targets, i.e. terrorist financing.	Training Lack of Expertise

16	Inaccurate and Incomplete transaction reporting	Reporting Transaction Process: failed to submit accurate transaction reports in respect of approximately 40 million transactions	Irresponsible behaviour: Staff had not submit the mandatory static data form to the External ARM so it had stopped transaction reporting on behalf of Credit Suisse	(SUP 17) - Inadequate controls in relation to transaction reporting, failures occurred during a period of heightened awareness around transaction reporting issues depicting corporate governance inefficiencies, Credit Suisse mistakenly assumed that 25% of its reportable transactions were being reported on its behalf by the External ARM but failed to develop and implement controls to confirm that those reports were being submitted, failed to impose controls to ensure that reporting is implemented according to the FSA requirements	Credit Suisse's failure to submit accurate transaction reports could have a serious impact on the FSA's ability to detect and investigate suspected market abuse and consequently could impact the FSA's ability to maintain market confidence and reduce financial crime, its failure has impaired the FSA's ability to provide accurate transaction reporting data to overseas regulators; the errors also create a serious risk of hampering other competent authorities' work in maintaining market confidence and of damaging the FSA's credibility within the EEA	Lack of controls

17	Unfair Customer Treatment	Failures occurred from errors from a 3rd party data producer as a result consumers being misled as to the true nature of the investments held by the Fund and, as a result, being given misleading information on the risk of capital losses, displaying on its website unclear and unfair marketing material	Employees raised concerns on the issues but no action was taken	(3, 7) - Inadequate systems or controls; to ensure that marketing material issued accurately reflected the investment strategy for the Fund, to investigate concerns regarding marketing material, resulting in a failure to promptly remedy failings after concerns were raised, internal reviews were too narrow and failed to identify failings properly, inadequate controls around the arrangements with the data producer, these control weaknesses extended beyond the Fund and related to all factsheets produced by the data producer, lack of data quality assurance, issue were not escalated to senior management- data producer continued to issue incorrect and misleading factsheets, ineffective communication between business areas and committees resulting in lack of awareness, business operated in distinct silos without any one having overall responsibility for ensuring that the marketing material correctly reflected the investments held by the Fund	-	Lack of Leadership

18	Unfair Customer Treatment	Sales Process and Complaints Handling Process Failure	Unintentional: Sales agents did not have the necessary skills and knowledge to prove customers with suitable advice as a result of recruitment, training and competency failures, commission attached to sales volume and not on quality of sales (lack of understanding)	(3, 6) - Failed to embed a culture focused on the importance of treating customers fairly, inadequate internal controls and governance arrangements to mitigate risks of unsuitable customer advise and unfair treatment of complaints, systemic failings; recruitment, training, competency, remuneration and reward, ineffective controls to manage risk of poor customer outcomes, lack of monitoring claims handling, incomplete documentation resulting to ineffective use of management information and root cause analysis to improve customer outcomes, ineffective governance arrangement and controls to identify and manage risk on TCF, ineffective actions when issues arose, TCF had been a priority for FSA since 2004 and governance failed to focus on this issue, the selling of additional policies to existing customers was a key aspect of CICA's business model, failure to mitigate the risk of inappropriate sales and sales representative behaviour inconsistent to TFC requirement	Presented a significant risk to the FSA's objective of securing protection for consumers	Training Remuneration Schemes

19	Unfair Customer Treatment	Sales Process Failure: Risk of mis-selling of financial products: 2,485 NHFA customers were advised to invest in asset-backed investment products (investment bonds) which were used to fund long-term care costs for elderly customers but failed to ensure the suitability of advice	Inappropriate- failure to assess customer risk profile that led to advisers recommend investment strategies inconsistent with their tolerance for risk, failure to recommend alternative products	(9) - the standard of supervision by the sales managers posed a high risk of customer detriment, systemic failings and persisted over a long period (5 years), inadequate sales process and standard of supervision and management control, inadequate procedures for monitoring the quality of sales which meant that the issues relating to the suitability of advice given to customers were not identified	NHFA was the leading supplier in the UK of independent financial advice on long-term care products to help pay for care costs, with a market share in recent years approaching 60%; HSBC is a major global financial services provider with a prominent position in the retail consumer market. The failures at NHFA highlight the need for regulated firms to ensure that where they acquire new businesses they implement appropriate systems and controls to manage and oversee their activities effectively. This includes positioning the new business in reporting structures that allow the wider Group to identify promptly and monitor any risks associated with new business. Where firms do not do this there is a significant risk of regulatory breaches, customer detriment and reputational damage.	Monitoring

20	Unfair Customer Treatment	Sales Process Failure: Failed to ensure that customers were suitably advised relative to the Fund for its customers	Unintentional: advisers were not provided with adequate training on the Fund and its features and risks were not sufficiently explained to them.	(9) - Inadequate training, inaccurate documentation of describing the Fund and its risks, failed to appropriately respond to the changing market conditions, ineffective compliance review of its sale and the Fund, inadequate monitoring, failings in relation to diversification, Failure to adequately investigate and address questions raised about past sales, failings existed for more than 4 years, failed to take appropriate action to address questions raised by a senior staff member relative to the Fund and its sales	The FSA has taken into account Coutts' size and financial resources. Coutts is a major private bank in the UK. As such, it has a leading competitive position in the market and its practices set an example for others in the financial services industry.	Training
21	Unfair Customer Treatment	Sales Process Failure: Customers were not advised suitably, according to their risk appetite as a result customers were exposed to an unacceptable risk of being sold a SCARP which was unsuitable for them	Intentional-it was the responsibility of the Team Leaders and Sector Heads to supervise the work of the Relationship Managers. However, Team Leaders also had responsibility for advising Customers of their own. Team Leaders and Sector Heads were responsible for overseeing all business activity within their respective business units which restricted their ability to oversee the work carried out by Relationship Managers	(3) - inadequate systems and controls in respect to the determination of customers' attitudes to risk as a result, there was an unacceptable risk that Credit Suisse UK may not have accurately understood the level of risk that customers were willing to accept from their investments, inadequate monitoring mechanisms to ensure that its staff took reasonable care to ensure the suitability of their advice	The FSA considered Credit Suisse UK's size and financial resources. It is one of the largest private banks in the UK with gross income of approx. £73 million (31 March 2011). During the Relevant Period, it advised on the sale of 1,701 scarps to 623 customers. The total value of scarps sold by Credit Suisse UK during this period exceeded £1.099 billion. As a result of its competitive position in the market, the firm's practices set an example which is seen by other market practitioners and customers. Thus, it is vital that it takes reasonable care to ensure the suitability of customer advice.	Monitoring

22	Risk of Bribery and Corruption	Staff conducted unethical activities associated with making commission payments totalling £27million to Overseas 3rd Parties who helped Willis Ltd win and retain business from overseas clients	Intentional: Unethical/ Irresponsible behaviour: staff in a large number of cases carried out insufficient due diligence prior to making payments, inadequate reporting by staff, lack of training and guidance concerning bribery and corruption	(3, SYSC 3.2.6R) - Inadequate commercial rationale to support payments to Overseas 3rd party, lack of formal training and brief description of the reasons for commission payment, inadequate documentation leading to inadequate monitoring of the effectiveness of its procedures, inadequate due diligence to evaluate risks involved contributing to a weak control environment giving rise to an unacceptable risk that payments made by Willis Limited to Overseas 3rd Parties could be used for corrupt purposes, including paying bribes to persons connected with the insured, the insurer or public officials, new anti-bribery and corruption policies were developed however, the Board did not receive sufficient relevant management information regarding their performance which would have allowed them to assess whether bribery and corruption risks were being mitigated effectively, relied on informal means to assess bribery and corruption risks, lack of information flow inducing problems to remain unrevealed, lack of regular monitoring	The involvement of UK financial institutions in (potentially) corrupt practices overseas undermines the UK financial services sector integrity. Unless they have in place robust systems and controls which govern the circumstances in which payments may be made to 3rd parties and then ensure those systems and controls are followed, UK financial services firms risk contravening UK and/or overseas anti-bribery laws. The FSA's financial crime and market confidence statutory objectives are both endangered by UK firms' failures in this regard. Willis Ltd is one of the largest insurance and reinsurance brokerage and risk management firms in the UK. As such, it has a leading competitive position in the market and the firm's practices set an example which is seen by other market practitioners and customers.	Training, Monitoring, Information Flow

23	Aggressive Growth Strategy with a specific focus on high-risk, sub-investment grade lending	Corporate Banking Division conducted an aggressive growth strategy despite known weaknesses in the control framework which means that it failed to provide robust oversight and challenge to the business	Unintentional: staff were incentivised to focus on revenue rather than risk which induced greater risk taking	(3) - Aggressive strategy continued despite market conditions worsening thus governance did not take reasonable steps to assess, manage or mitigate the risks involved in the aggressive growth strategy, failed to take reasonable care to ensure that Governance adequately and prudently managed high valued transactions which showed signs of stress, culture was focused on revenue rather than on risk adjusted returns thus incentive mechanisms encouraged behaviours such as; increasing risk appetite, optimism at the expense of prudence, regarding risk management as a constraint on the business rather than integral activity, issues on the quality, reliability, utility of available management information affecting the effectiveness with which the risks of the business could be assessed, managed and mitigated, inefficient oversight, issues with quality and scope of assurance work, board disregarded warning from divisional function and HBO's auditors, high degree of reliance on relationship managers, subject to management supervision and oversight, with regard to credit analysis and due diligence; relationship managers dealing in lower value transactions were delegated significant power to extend further credit to existing customers, subject to management supervision and oversight; resistance to change impeding any efforts to improve control framework and prioritise risk management, risk appetite was not defined	These failings had, or might reasonably be regarded as likely to have had, a negative effect on confidence in the UK financial system	Incentive Schemes

24	Unfair Customer Treatment: unsuitable advice provided to the customers	Sales Process Failure, Mis-selling of products: Inadequate information was given to customers regarding the products by staff operating out of Barclay's retail branches	Training material was inadequate, failed to make staff aware about the suitability of the products to the customers , sales briefs and product updates referred only to benefits of the product, consideration of the risks attached to it were not submitted	(9) - inadequate monitoring of sales procedures resulting into a failure to promptly identify and investigate potentially unsuitable sales, compliance monitoring identified particular but governance failed to take appropriate and timely action to address them in its sales process and a number of unsuitable sales were made, concerns were raised by the customers but failed to take any action, failure in training of advisers, deficient training material and inaccurate documentation given to the advisers concerning the selling products without specifying the type of risk profile these product should be sold to, thus training advisers were giving a misleading impression of the risks involved, inadequate sales process and procedures supervision, absent compliance controls	-	Training

25	Unfair Customer Treatment	Complain Handling Process Failures: It received 1.1million complaints in 2009	Complaint handlers did not have the necessary competence to manage customers' complaints and did not always follow the prescribed process: inadequate guidance and training, lack of product knowledge, lack of formal arrangements for cascading decisions meaning that information was not communicated consistently and complaint handlers dealing with routine complaints at the front line were not always aware of and did not always take account of FOS decisions when deciding complaints	(3, 6) - Monitoring at branch level and the resulting management information produced was ineffective in assessing whether customers were being treated fairly, controls focused on measuring whether complaint handlers dealt with complaints within target time frames rather than the quality of the process. Inadequate investigation with complaint handlers failing to obtain all the relevant factors when investigating complaint, limited training on complaint handling, failures existed for 2.5 years, although governance was aware of the failures in the complain handling process it failed to undertake appropriate actions, ineffective monitoring of the quality of complaint handling at branch level thus poor behaviour was undetected, management information provided to senior management regularly highlighted the ongoing issue of complaint handlers failing to attach on the complaint handling management system the mandatory acknowledgment and resolution letters	RBS UK Retail is the second largest provider of retail banking products and services in the UK with approx. 2,200 bank branches and 15 million customers during the Relevant Period. The majority of consumers make complaints through the branch network, which, as the first point of contact, in most cases retained responsibility for resolving any complaint received. Therefore, given the nature of the failings there is an unacceptably high risk that customers may not have been treated fairly	Training

26	Misconduct relating to the calculation of LIBOR and EURIBOR undermining the integrity of the benchmark references	UBS, acting through its managers and employees, sought to manipulate certain LIBOR currencies and EURIBOR in connection with the submission of rates that formed part of the calculation of LIBOR and EURIBOR to benefit trading positions	Unethical illegal behaviour - employees involved in the misconduct were recklessly and frequently deliberate: manipulation of UBS' own submission involved (all currencies departments combined) 47 individuals where 17 of them were Managers. Trader submitters influenced the submissions they made to suit their own trading position. Manipulation in collusion with brokers and other banks: UBS Trader colluded with individuals at Panel Banks to make submissions that benefited UBS' trading positions, facilitation trades (wash trades) and illicit transactions were used to incentivise and reward counterparts.	(3, 5) - Numerous UBS managers knew about the incident and some were actively involved in LIBOR and EURIBOR manipulations. In total, improper requests directly involved approx. 40 individuals at UBS, 11 of whom were Managers. At least two further Managers and five Senior Managers were also aware of the practice of the manipulation of submissions to benefit trading positions. The practice of attempts to manipulate LIBOR and EURIBOR submissions to benefit trading positions was often conducted between certain individuals in open chat forums and in group emails, which included at least a further 70 individuals at UBS. Absence of systems, controls or policies governing the procedure for making LIBOR EURIBOR submissions, inadequate review, the new procedures were inadequate in their design and further were inadequately implemented. Management failed to manage the business areas appropriately, these failings were not detected by Compliance nor Group Internal Audit	UBS's breaches of Principle 5 were extremely serious. Its misconduct gave rise to a risk that the published LIBOR and EURIBOR rates would be manipulated and undermined the integrity of those rates. In addition to its routine internal manipulation of its own LIBOR and EURIBOR submissions, UBS's collusion with Panel Banks and Brokers significantly increased the risk of manipulation of the published JPY LIBOR rates because the averaging process applied to submissions as part of the calculation of the published rate means that the risk of manipulation is greater if more than one Panel Bank's submission has been manipulated. UBS, and in particular its investment bank, is one of the biggest, most sophisticated and well-resourced financial services institutions in the UK. Serious breaches committed by a firm such as UBS merit the highest penalties	Absence of Controls Lack of Internal Audit Inadequate systems review

27	Rogue Trader	Rogue Trading incident: Kweku Adoboli on the Exchange Traded Funds Desk in the GSE trading division had amassed substantial losses amounting to $2.3 billion through his trading	Illegal unethical behaviour: fraud of market abuse and false accounting	(3, 2) - Insufficient focus on the key risks associated with unauthorised trading within the GSE business resulting into significant control breakdowns allowing concealment to remain undetected for a long period, failed to adequately supervise the GSE business with due skill, care, diligence. Inadequate systems and controls in place to detect the unauthorised trading in a timely manner, inadequate focus on risk management systems and to sufficiently escalate or take sufficient action in respect of identified risk management issues, failed to: provide appropriate level of supervision, challenge appropriately the employees in question, implement effective remedial measures in response to several warning signs that occurred during the course of its business, put in place systems and controls to adequately mitigate the risk that its employees would undertake unauthorised trading and where such unauthorised trading was carried out, to detect the trading in a timely manner, inadequate systems and controls for countering the risks posed by unauthorised trading	Market confidence was put at risk, given the sudden announcement to the market size and the losses announced. Negative announcements such as this, put a real risk the confidence investors are prepared to have in financial markets.	Supervision

28	Unfair Customer Treatment: Mis-selling of products for nearly 7 years	Sales Process promoted an excessive focus on sales, revenue, and commercial objectives at the expense of treating customers fairly	Unintentional: Sales advisers were inappropriately seeking to persuade customers to buy insurance cover, which they did not need, on the basis that customers could cancel them during the 'cooling-off' period, while they pursued inappropriate objection handling techniques to discourage customers to cancel their policies	(3, 6, 7) - despite being alert by FSA CPP continued to pursue this sales approach, failed to identify issues in the sales control, corporate governance provided: lack of acceptance in the Compliance report 2007, conflicting information about decision making in the firm as it was unclear which body took decision CPP or the UK leadership team-the UK leadership team was not a formal body and the matters discussed and decisions taken were not recorded. Compliance oversight, firm's practices did not match its documentation, the board was aware of these failings but failed to take sufficient action to deal with them	-	Training
29	Mortgage Systems relied upon incorrect records for 8 years-customers were not receiving important information, thus making insufficiently informed decisions about their mortgage accounts	Errors existed in the information held on BOS mortgage systems which resulted from an inadequate systems integration and from manual processing errors, systems were not consistently integrated and properly synchronised generating incorrect mortgage offer letters to customers	Manual Error: Staff required to manually updating the Borrowers System to reflect the new Version. However, this manual change was not always effected and as a result approximately 60,000 customers' details were not updated on the Borrowers System	(3) - failed to identify errors that led to inaccurate information being held on its mortgage systems, errors were only identified after customer complaints rather than through internal systems. Errors occurred from inadequate systems integration and manual processing errors	-	Lack of Manual systems control

30	Misconduct relating to its submission of rates which formed part of the LIBOR EURIBOR setting process: Barclays inappropriately accounted for its Derivatives Traders position when making US dollar LIBOR and EURIBOR submissions for 5 years	External Factor: Media and negative publicity against its low LIBOR submission raising questions whether its submissions indicated liquidity problems induced senior management to give instructions to lower senior managers to reduce LIBOR submissions to avoid negative publicity	Unethical, Illegal: Inappropriate submissions requested by derivatives traders (including requests made from derivatives trader at other banks) motivated by profit seeking to benefit Barclay's Trading Positions. There were at least 14 Derivatives Traders including senior Derivatives Traders. Trading Desk Managers received or participated in inappropriate communications, internal traders were completing favours of external traders- unclear guidelines about the importance of the integrity of the process, lack of training about submission process and appropriateness of requests for favourable submissions	(2, 3, 5) - Failed to observe proper standards of market conduct when making US dollar LIBOR and EURIBOR submission. Systems and control failings: no specific systems and controls in place relating to its LIBOR and EURIBOR submissions processes, compliance failings, and LIBOR issues were escalated to Barclay's Investment banking compliance function where compliance failed to asses and address the issues effectively, compliance failure let to unclear and insufficient communication about issues to the FSA. Senior managers were more concerned over negative publicity perception over LIBOR submission than efficiency of internal controls. System and Control Failures: inadequate monitoring of the submission process, no spot checks on the level of actual transactions in the interbank market, lack of integrity review, lack of understanding the risks of submission process, unclear lines of responsibility for systems and controls, lack of guidance concerning internal or external inappropriate communications, senior manager raised concerns about potential of conflict of interest between Submitters and derivatives traders but compliance took no action, compliance failed to report the issues at the FCA	Where Barclays made submissions which took into account the requests of its own Derivatives Traders, or sought to influence the submissions of other banks, there was a risk that the published LIBOR and EURIBOR rates would be manipulated. Barclays could have benefitted from this misconduct to the detriment of other market participants. Where Barclays acted in concert with other banks, the risk of manipulation increased materially	Monitoring

31	Failures in corporate governance and control arrangements resulting in poor organisation and management across its business as a whole following a decision to expand and diversify into a new business area, by writing business for European clients through three branches across Europe.	Developing operations failures: Decision to change business strategy	Unintentional: Rotational staffing strategy (typically 3 years): personnel with limited experience, skills and knowledge on the new area were placed in senior positions, CEO appointed at a critical stage-expansion strategy with lack of experience, personnel was unfamiliar with UK regulatory environment, understaffing, limited training on arrival however lack of relevant skills and experience remained	(3) - Failed to consider FSA warning on the importance of careful and focused board oversight which requires good systems and controls. Corporate governance, Directors and senior management failed to take the appropriate measures in a timely manner, weak board effectiveness, lack of corporate behaviour on the board, failed to operate at the level appropriate for the size and complexity of developing operations, inadequate oversight and controls and insufficient resources, governance focused on profitability of the new business without taking effective actions to ensure that governance and system and controls complied with UK regulation, insufficient capital reserves, inappropriate segregation of duties and responsibilities especially relating to the Three Lines of Defence which was compromised, responsibility for functions within different Lines of Defence was not always allocated to different individuals, ineffective IT systems implementation resulting into inadequate and poor quality of management information which made it unable to control business written in its branches, failings undermined senior management's ability to monitor and control its branch, lack of leadership, failed to ensure that duties and responsibilities were appropriately divided between senior members of staff, and took inadequate steps to ensure that individuals were not given too wide a span of responsibility, senior management was aware about weaknesses but failed to respond effectively and failed to appreciate risks associated with their actions/non-actions	-	Rotating Staff scheme, Training, Lack of Experience and Skills

32	Money Laundering	Insufficient customer information about their profile and poor assessment of customer riskiness to reduce the risk of the bank being used for money laundering	Process Design: Staff were incentivised to increase the customer base without focusing on the customer quality, lack of proper training affecting the gathering of due diligence information, lack of guidance regarding customer information gathering and assessing the source of customer funds	(3, SYSC) - Inadequate risk assessment of the risk of money laundering, failed to gather the appropriate level of due diligence information about high-risk customers, to apply robust controls when establishing relationships with high-risk customers, inconsistent and inappropriate level of monitoring to its existing customers to identify, assess and manage, their risk profile, inadequate reviews of its systems and controls, relevant customer information was not kept up-to-date, failings persisted for 3 years and were not identified by the firms, failing occurred in a period of awareness concerning this issue but governance failed to take the necessary steps, lack of appropriate challenge to the bankers, decision made by senior managers were based on the limited information and poor assessment of the bankers' results, lack of senior management oversight and transaction monitoring, inadequate scrutiny of customer transactions, insufficient reviews for governance to remedy the deficiencies	The laundering of money through UK financial institutions undermines the UK financial services sector. It is the responsibility of UK financial institutions to ensure that they are not used for criminal purposes and, in particular, that they do not handle the proceeds of crime. Coutts is a high profile bank with a leading position in the private banking market and is a gateway to the UK financial system for high net worth international customers. It was particularly important, therefore, that Coutts had robust systems and controls to prevent and detect money laundering.	Incentive Schemes
33	Risk of Mis-selling products	Sales process Failure: Insufficient information provided to investors about structured products that may have caused decisions to be made without understanding the limitations of cover offered for those products	Unintentional: insufficient training material relative to structured products-did not explain circumstances where cover would be available	(2, 7, Rule 6.1.16) - Failed to clarify properly and conduct full analysis of the scope of FSCS coverage despite that management was aware that did not have full understanding of the positions. Inadequate steps to ensure its sales advisers were aware of the extent of FSCS coverage and properly communicated that information to investors	-	Training

34	Employee submit altered documentation	FSA received files which have been altered improperly-FSA requires information it requests from firms to be submitted in the original state and not altered	Intentional inappropriate induced by management instructions: staff altered staff altered the files that had to be submitted to FSA in order to avoid disciplinary actions	(2) - Inadequate systems to ensure that files requested by FSA were not improperly altered as a result of failure occurred in the fine review. Management failure: Prior to the start of the earlier exercise, management had told staff during a conference call that if they were found not to be operating to the required standards, they would face internal disciplinary investigation. This message to staff increased the risk that files would be altered improperly. Failed to take robust steps to ensure that the FSA receives accurate information.	Submitting altered information undermines the FSA's ability to supervise effectively the financial services sector and meet its objectives of protecting consumers and promoting market confidence; and the Firms are part of RBS Insurance which is a prominent institution with significant operations in the UK. RBS Insurance is the second largest general insurance provider and the largest personal insurer in the UK. The size and potential consumer impact of RBS Insurance's operations require a significant degree of supervision from the FSA. The FSA relies on the receipt of accurate information from RBS Insurance in order to supervise its operations effectively.	Management Failure Wrong incentives

Appendix 4: Reaction to an Incident

(The shades indicate similarities across the cases)

Case	Incident	Reaction at Operational Level	Reaction at Managerial Level
7	Recognised	No action	Ineffective action by managers
15	Recognised	No action	Ineffective action by managers
28	Recognised by FSA	No action	Aware about failures but no action was taken
29	Recognised only after customer complaints	No action	No action
20	Recognised	Senior Member raised awareness	No action
23	Recognised by auditors	Divisional levels raised awareness	No action
4	Recognised	Slow information flow along the hierarchy	Failed actions
12	Recognised	Action initiated by employee	Aware about failures but no action was taken
17	Recognised	Employees raised awareness	No effective actions resulting from miscommunication and silo operations
14	Recognised by Internal Review a year later	Action initiated by employee	Could be avoided if managers took action to FSA's warnings
26	Unrecognised	Action initiated by employees	Managers were also involved in the illegal actions
3	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
5	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
8	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
9	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
13	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
16	Unrecognised	No action	Could be avoided if managers took action to FSA's warnings
18	Unrecognised	No action	Could be avoided if managers implemented controls in accordance with FSA's requirements
31	Unrecognised	No action	Could be avoided if managers took action to FSA's warnings
32	Unrecognised	No action	Could be recognised if management took action to FSA's warnings
6	Unrecognised	No action due to inexperienced staff	No action
10	Unrecognised	No action	No action
11	Unrecognised	No action	No action
1	Unrecognised	No action	No action
2	Unrecognised	No action	No action
19	Unrecognised	No action	No action
21	Unrecognised	No action	No action
22	Unrecognised	No action	No action
24	Unrecognised	No action	No action
25	Unrecognised	No action	No action
27	Unrecognised	No action	No action
30	Unrecognised	No action	No action
33	Unrecognised	No action	No action
34	Unrecognised	No action	No action

Appendix 5: Causes of Behaviour and Employee Intentions

(The shades indicate similarity across the cases)

Case	Causes of behaviour	Intentional or Unintentional
12	Lack of controls	Intentional
26	Lack of controls	Intentional
2	Incentive Schemes	Intentional
34	Incentive Schemes	Intentional
19	Monitoring	Intentional
30	Monitoring	Intentional
6	Supervision	Intentional
7	Supervision	Intentional
14	Supervision	Intentional
27	Supervision	Intentional
22	Training and Monitoring	Intentional
23	Incentive Schemes	Unintentional
32	Incentive Schemes	Unintentional
17	Lack of leadership	Unintentional
13	Managerial Negligence	Unintentional
1	Training	Unintentional
3	Training	Unintentional
4	Training	Unintentional
7	Training	Unintentional
15	Training	Unintentional
24	Training	Unintentional
25	Training	Unintentional
28	Training	Unintentional
31	Training	Unintentional
33	Training	Unintentional
14	Training	Unintentional
20	Training	Unintentional
6	Training (of the back office)	Unintentional
5	Training and Incentive Schemes	Unintentional
18	Training and Incentive Schemes	Unintentional
8	Training	Unintentional but inappropriate
9	Training	Unintentional but inappropriate
10	Training and Monitoring	Unintentional but inappropriate
11	Training and Monitoring	Unintentional but inappropriate
21	Monitoring	Unintentional but irresponsible
29	Lack of manual system controls	Unintentional but irresponsible
16	Lack of controls	Unintentional but irresponsible

Appendix 6: Causes of Failure at the Institution Level

(The shades indicate similarity across the cases)

Case	Cause of Failure
3	Corporate Governance
5	Corporate Governance
6	Corporate Governance
8	Corporate Governance
9	Corporate Governance
12	Corporate Governance
13	Corporate Governance
14	Corporate Governance
15	Corporate Governance
16	Corporate Governance
34	Corporate Governance
25	Corporate Governance
28	Corporate Governance
33	Corporate Governance
4	Organisational Culture
7	Organisational Culture
18	Organisational Culture
19	System and Controls
1	Systems and Controls
2	Systems and Controls
10	Systems and Controls
11	Systems and Controls
21	Systems and Controls
27	Systems and Controls
29	Systems and Controls
32	Systems and Controls
23	Corporate Governance, Organisational Culture
22	Organisational Culture, Systems and Controls
17	Systems and Controls, Organisational Culture
24	Systems and Controls, Corporate Governance
31	Corporate Governance, Systems and Controls
30	Systems and Controls, Corporate Governance, Organisational Culture
26	Systems and Controls, Corporate Governance, Organisational Culture
20	Corporate Governance, Organisational Culture, Systems and Controls

Appendix 7: Impact of People Behaviour in the Industry

(The shades indicate similarity across the cases)

Case	Impact of People Risk
18	Customer Protection
8	Customers Protection
9	Customers Protection
16	FSA's ability to maintain Market confidence and reduce financial crime
26	Direct Impact
30	Direct Impact
15	Integrity of FSA
22	Integrity of FSA
32	Integrity of FSA
34	Integrity of FSA
10	Integrity of FSA, Market Confidence and Financial Crime, Size
14	Material Risk to the FSA's objectives
4	Market Confidence
6	Market Confidence
13	Market Confidence
23	Market Confidence
27	Market Confidence
2	Size
12	Size
20	Size
21	Size
25	Size
19	Size, Stricter Regulation
3	Stricter Regulation
1	-
5	-
7	-
11	-
17	-
24	-
28	-
29	-
31	-
33	-